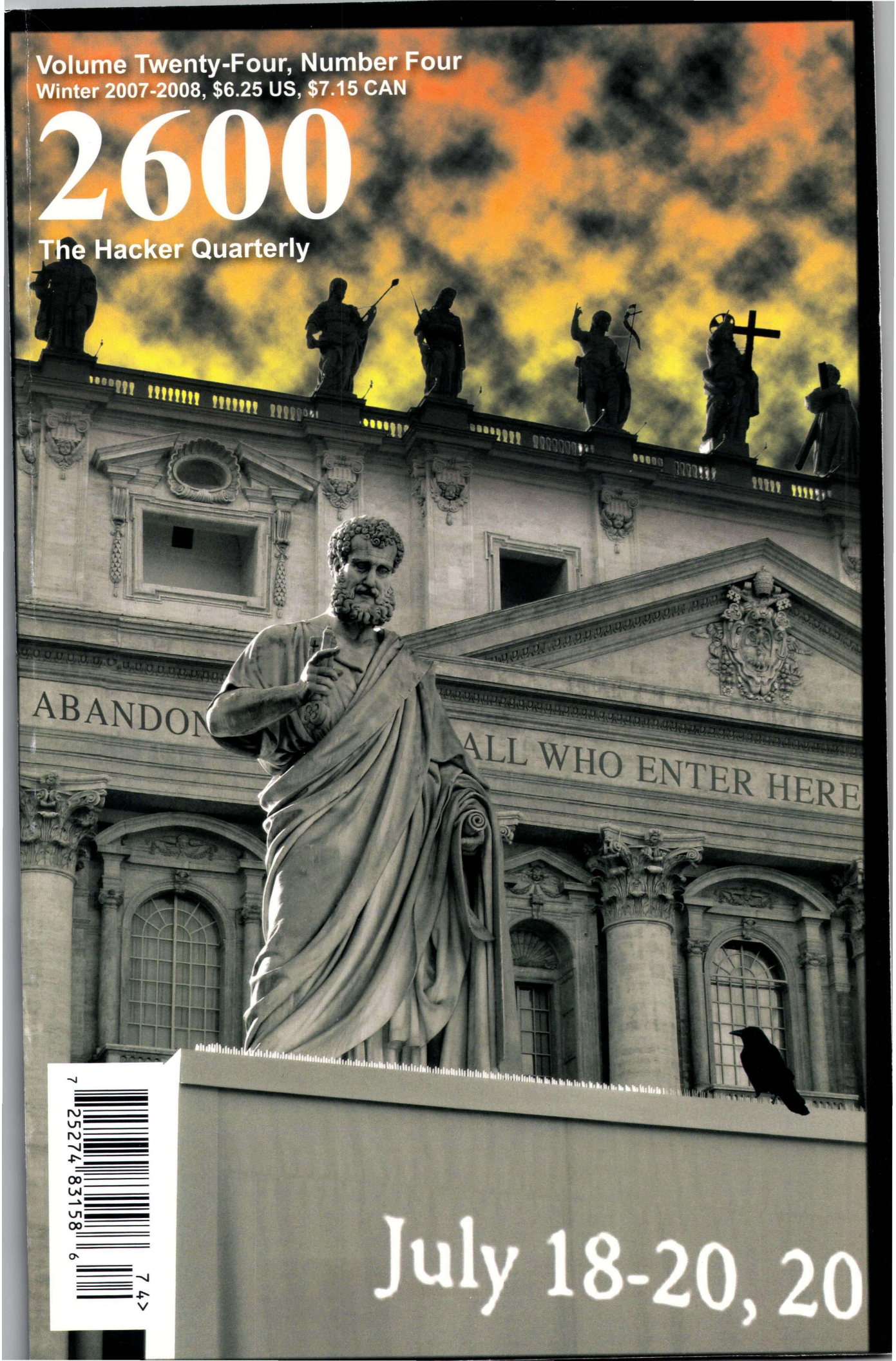
Volume Twenty-Four, Number Four
Winter 2007-2008, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



Payphones of the Americas

United States. One of the more creative payphones of the States, found (where else?) at the entrance to the Kennedy Space Center on Merritt Island in Florida.

Photo by icurnet

Costa Rica. Seen at a local shopping mall. Note how large the phone number is on this particular model. It's almost as if they want people to call payphones, unlike in the States where incoming service is often turned off.

Photo by RadioRover

Belize. Found in a restaurant/bar in San Ignacio. What it lacks in size it makes up for in overall design.

Photo by Phred

Colombia. Seen in Chia, this bank of phones has what has to be the most dramatic awning ever made for payphones.

Photo by Random

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

Presentations

The More Things Change...	4
Power Trip	6
Building Your Own Networks	9
Pirates of the Internet	11
Telecom Informer	13
Darknets	15
Scanning the Skies	16
Essential Security Tools	18
Decoding Experts-Exchange.com	20
An Introduction to Beige Boxing	21
Hacking the SanDisk U3	22
Exploring AT&T's Wireless Account Security	24
Hacker Perspective: Rop Gonggrijp	26
(More) Fun with Novell	29
PayPal Hurts	30
Facebook Applications Revealed	32
Letters	34
Hacking Windows Media DRM	48
The Noo World	49
Forensics Fear	51
Transmissions	52
Cracked Security at the Clarion Hotel	54
Building Your Own Safe, Secure SMTP Proxy	55
Zero-Knowledge Intrusion	57
Booting Many Compressed Environments on a Laptop	58
Avoid Web Filtering with SSH Tunneling	61
Marketplace	62
Meetings	66

The More Things Change...

As we move towards our 25th year of publishing, we find that so much has changed in the world we write about. Yet somehow, a surprising amount of things are almost exactly the same.

Let's look at where technology has taken us. Obviously, nothing has stood still in the hardware and software universe. In 1984, ten megabytes of storage was still more than what most people had access to. Those few who even had their own computers would, more often than not, wind up shuffling five and a quarter inch floppies before they would invest in an expensive piece of hardware like a hard disk. And speed was a mere fraction of a fraction of what it is today. If you could communicate at 300 baud, it was considered lightning fast to most people. Of course, there were those who were always pushing to go faster and get more. It was this incessant need for expansion and improvement that got us where we are today.

Perhaps not as dramatic in scale but certainly as wrenching in feeling has been the change to our society and the world around us. In the current day, we are security-obsessed without having gotten any better at being secure. We seem to have lost any semblance of the trust that once guided us as human beings. Instead, we live in a state of perpetual alertness, suspicion, and fear. Some would say that this is reality and that this state of mind is the only way to survive in a hostile world. We would say that it's a sad reality and one that needs to be analyzed and hopefully altered. Were we to have started publishing in 2008 rather than in 1984, we likely would have been quickly branded as potential terrorists before ever being able to establish a foothold in our culture that enabled us to be seen as a revealing and even necessary voice.

Today we continue to exist in no small part because we have existed for nearly a quarter century. It is that history which strengthens us and one we should all try and learn as much as we can from.

So what has managed to stay the same over the years? A number of things actually, some good and some bad.

For one, the spirit of inquisitiveness that drives much of what the hacker world consists of is very much alive and in relatively the same state it's been in for so long. If anything were to sum up what every single one of our articles has had in common over all these years, it's that desire to find out just a little bit more, to modify the parameters in a unique way, to be the first to figure out how to achieve a completely different result. Whether we're talking about getting around a barrier put in place to prevent you from accessing a distant phone number or a restricted computer system, or cracking the security of some bit of software so that you can modify it to perform functions never dreamed of by its inventors, or revealing some corporate secrets about how things really work in the world of networks and security - it's all about finding out something and sharing it with anyone interested enough to listen and learn. These are the very foundations upon which *2600* was founded and those values are as strong today as they were back in our early days. In many ways they have actually strengthened. The Internet is an interesting example of this. While its predecessor, the ARPANET of the 60s and 70s, was developed under the authority of the military, what has evolved since then is a veritable bastion of free speech and empowerment of individuals. Of course, it's not all so idealistic. Not everyone cares and there's a constant struggle with those who want the net to be nothing more than a shopping mall and those who seek to control every aspect of it. But who can deny that literally any point of view can be found somewhere on today's net? And a surprising amount of people will defend that concept regardless of their own personal opinions. Almost without fail, if someone is told that they may

not put forth a certain viewpoint or spread information on a particular subject, then the community of the net will respond and make sure the information is spread more than it ever would have been had there not been an attempt made to squash it in the first place. Nobody has yet been able to put the top back on the bottle and prevent this kind of a reaction since never before in the history of humanity has such a tool been so widely accessible. There obviously is still a long way to go and a good many battles to fight in order to keep free speech alive on the net. But this is at least encouraging and indicative of how hacker values have easily meshed with more mainstream ones.

But something else which hasn't changed over the years is the malignment of hackers and what we stand for. The irony is that most people understand perfectly well what we're all about when presented with the facts. The mainstream media, however, never has and probably never will. It's simply not in their interests to portray us as anything but the kind of threat that will help them sell newspapers and get high ratings. Fear sells - that is the unfortunate truth. And fear of the unknown sells even better because so little evidence is needed to start the ball rolling.

In the media, as in politics, enemies are needed in order to set forth an agenda. From the beginning, hackers have fit the qualifications to be that enemy. They know too much, insist on questioning the rules, and won't stop talking and communicating with themselves and others. These types of people have always been a problem in controlled environments like dictatorships and public schools. It's not too difficult to see why they're viewed with such hostility by people who want to hold onto whatever power they happen to have. A true individual is no friend to autocrats.

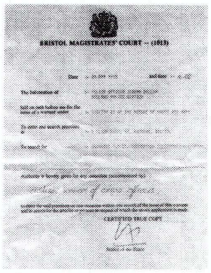
If you read a newspaper or watch virtually any newscast, you won't have to wait too long for a story to appear with details on how the private records of thousands (or sometimes millions) of people have been compromised while in the care of some huge entity. We could be talking about a phone company, credit card provider, bank, university, or government. And the information that was lost might include anything from people's names, addresses, unlisted phone numbers, Social Security and/or credit card numbers, a list of purchases, health records, you name it: data that was entrusted to the company, agency, or bureaucracy for safekeeping which has been compromised because someone did something foolish, like somehow post confidential hospital files to a public web page, or copy customer information to a laptop which was subsequently lost or stolen. Yet in virtually every instance of such a profound gap in common sense, you will find that hackers are the ones getting blamed. It makes no difference that hackers had nothing to do with letting the information out in the first place. The media and the authorities see them as the people who will do virtually anything to get private data of individuals and make their lives miserable.

This misdirection of blame serves two purposes - as it always has. The first is to absolve those really responsible of any true blame or prosecution. The second is to create an enemy who can be blamed whenever anything goes wrong. Of course, the irony is that if hackers were the ones running and designing these systems, the sensitive data would actually be protected far better than it is now. There simply is no excuse for allowing people's private information to be copied onto insecure machines with no encryption or other safeguards. The fact that it keeps happening tells us that dealing with this isn't very high on the priority list. Perhaps if those organizations that don't have sufficient security practices were held accountable rather than being allowed to blame invisible demons, we might actually move forward in this arena. But one must ask what would be in it for them? The answer is not a whole lot.

These battles and conflicts will no doubt continue regardless of what direction our society takes us. While we have indeed been frustrated with the seeming lack of progress on so many levels, we can't help but be fascinated with where we will wind up next - both in the technological and political spectrum. The combination of the two may very well seal our future for quite a long time to come.

The one thing that will keep us going (and that has made it so worthwhile for all of these years) is the spirit of curiosity that our readers and writers continue to proudly exhibit. It's a very simple trait, and perhaps one that's an unerasable ingredient of our humanity. It will survive no matter how our technology advances, regardless of any law or decree put forth to stifle it, and in spite of misperceptions and overall cluelessness. If we keep asking questions and thinking outside the box, there will always be something good to look forward to.

Power Trip



by OSIN

It is common in *2600* for writers to preface whatever topic they may be discussing with a disclaimer such as "I by no means condone or encourage illegal activity." That ends with this article. Since it is now impossible in America to tell who is a criminal and who is not, or to tell what is a crime and what is not, I wholeheartedly condone the practice of the actions I'm about to lay out by any and all criminals reading this article. But not to worry: should any of you criminals out there run afoul of the greatest crime syndicate since the Gambinos, you can always use the "Scooter" Libby lame-ass defense, assuming you're a rich, white, non-violent, first time offender.

One of the most used weapons of today's organized crime syndicate is the secret warrantless search. That means they can enter your residence while you're away and either seize computer equipment or bug the place. Surely such evil doesn't exist in the Land of the Free and Home of the Brave! And, how ironic: I began writing this article on the 4th of July. But, yes, things are taking place that I'm pretty sure the forefathers of the USA didn't intend. So, let's take a bite out of crime!

Our first weapon against evil-doers is wireless technology, specifically an Internet-capable wireless camera and a wireless access point (WAP). I won't go into the security considerations of wireless cameras and access points; I'll only say that it is in your best interest to change the default login password. There are many more security issues pertaining to this technology, but they are beyond the scope of this article. I strongly suggest that you educate yourself about these issues lest you give criminals access to spy on you. No, what we're more interested in at this stage are the capabilities of the wireless cameras on the market now. Different cameras have different capabilities, but if you were to select one, I would say it should have at least two capabilities: the ability to be monitored over the Internet with a browser and the ability to send email alerts or attachments.

You should consult your particular camera's documentation for information on how to set it up. I can't really give specifics since different manufacturers' cameras vary widely, but in most cases you can set the email notification, whether to send an mpeg attachment, the number of seconds to record, which email addresses to send the alert to, and so on. You should also think about such things as the placement of the camera. Set it far enough away from the area you're monitoring so that the camera has enough time to record a few seconds and send an email before it gets unplugged. You might even want to consider hiding it or disguising it as another object. The point is that you can't have a secret warrantless search if there's video of someone in your residence. And knowing about it is half the battle. Remember that they don't have to kick down your door or pick the lock. Many of these gangs have huge amounts of technical resources, so they can make their own keys to get into your place.

But let's not stop there; evildoers always collude with other criminal elements of society to get what they want. Anyone desperate enough to do a secret warrantless search is probably wise enough to case out the victim before such a search is actually conducted. And, during the course of such an investigation, they might discover that you have wireless cameras throughout your residence. How might they react? Well, barring a full-scale search and seizure, which would make secrecy moot, they might collude with a well-known criminal enterprise that shakes down citizens on a monthly basis: the power company. Keep in mind that the power company will always do what it takes to please its regulatory master. So, with no power, our wireless camera and setup is useless, right? Not so fast. Consider our second weapon against secret warrantless searches: the UPS.

When the UPS first came out, it was nothing more than a glorified surge protector. The first ones could power a desktop computer and monitor for about 15 minutes, really only useful to give the user time to gracefully shut down the computer. About a year ago, though, I came across the newer versions. They had a USB port which allowed them to be monitored with proprietary software on a laptop. They also boasted far greater power capacity than older models did. The one I bought could power a desktop and flat screen monitor for nearly 90 minutes. But, because I haven't used my desktop in years and I didn't want a good UPS go to waste, I wondered how long this UPS would power my wireless camera, broadband modem, and WAP. The power requirements for all three added up to 110 Watts while the UPS boasted an ability of 450 Watts. On top of being a surge protector, the UPS also contained a voltage

regulator so I had some confidence that using it outside its intended design parameters wouldn't fry my wireless setup. I gave it a go. Using my laptop to monitor the UPS I found that after an hour of running all three devices off the UPS, the battery's charge had fallen to around 92 percent. Not bad. Now, theoretically, if the power usage is linear, then that might run the setup for more than 10 hours, but in a real-world scenario, more power is going to be utilized as my wireless components become more active or have to send out data over my broadband connection. I never tested how long it could power the setup since you can decrease the life of the rechargeable 12 volt battery if you go below 80% charge, so let's assume for argument's sake that my UPS will power the full requirements of my wireless setup for 7 hours. That's still a long time for miscreants to have to wait to start their search.

But power outages are common in the United States. It's not unusual for one to occur, and there are usually no sinister forces behind them, so how do you know if the power outage at your residence is a normal one? For that matter, how would you know that one occurred? It's true that my UPS starts beeping when the power goes out, and since my wireless camera also has a microphone, I'd be able to hear it if I logged in to see what's going on. But I'd have to know that an outage has occurred to connect in the first place. The point is that you may not know if the outage is just a normal blackout, but there are ways of knowing that an outage has occurred. The problem is one of notification. And in this next part, I'm going to use a program that's been used on computers for several years to track battery energy consumption (our third weapon): Advanced Power Management (APM).

APM is normally used on laptops to monitor the battery and do some notifications when the battery level approaches critical levels. The good thing about APM is that it will tell you when the power goes out or the power adapter is unplugged from the wall socket. It goes without saying that APM will treat a power outage the same way it would treat unplugging the power adapter from the wall and running on battery power. For this example, I'll be using OpenBSD. On OpenBSD 3.9, my version of APM will give human readable statistics on the status of the power. On a laptop, the command to execute is `apm -v`. You may need to start the apm daemon first, which is merely `ampd`. When you run the `apm -v` command it will output three lines similar to these:

```
Battery state: high, 100% remaining,
151 minutes life estimate
A/C adapter state: connected
Performance state: uninitialized (200MHz)
```

But when the AC adapter is unplugged or there is a power outage the second line in the output from apm changes to this:

```
A/C adapter state: not connected
```

So, it's that particular line that we are most interested in. After plugging the laptop into a wall socket, we could write a script that would run in cron every minute and test whether that second line had changed. Before we proceed, though, I want to return to the wireless camera.

Anyone who has one of these cameras and has used the motion detection email attachment option will tell you that it's sometimes too sensitive to light changes and not sensitive enough to motion unless you have the sensitivity set to high. The false positives the camera sends out can be annoying. Wouldn't it be nice if the camera's motion detection option could be turned on only if the power goes out? I found that it is possible, assuming your camera allows it. Most of these cameras are running a simple web server to which you can log in and make changes to the settings and options. My camera, for instance, uses the GET method when you click the Apply button to turn motion detection and emailing on. The entire call I need to use shows up in the browser URL location bar. So now that I know what the full URL is to do this manually, I can incorporate that knowledge in my cron script so that when a power outage is detected it will automatically turn on the motion/email option using wget. Here is a Perl script that would perform this feat (the wget line has been truncated since the real call is very, very long):

```
#!/usr/bin/perl
@apm=`/usr/bin/apm -v`;
foreach $line (@apm) {
        if((index $line,"not
➥connected") > 1) {
#if the apm.lock file does not exist
                if (!(-e 'apm.lock')) {
# We only want this command to run
➥once which is why we have a lock file
                `wget -O powertrip.html
➥-http-user=admin -http-
➥passwd=yourpassword http://camera_ip/
➥adm/file.cgi?audio_enable=enabled&mo
➥t=enabled&email=you@yourisp.com"`;
                $lock=`/
➥bin/touch apm.lock`;
        }
        } else {
#The power is back on. Remove the lock
➥file but do not turn off monitoring
                if((index
➥$line,"connected") > 1) {
        $exec=`/bin/rm -f apm.lock`;
                }
        }
}
```

As I said, the http call has been severly truncated. The actual call is much longer. Each camera is different, though, so you may actually have to sniff your traffic to learn the actual call to your camera's webserver to turn on motion detection. Note that the variable that actually turns on monitoring is "mot" for my camera. To turn off monitoring, you would just change your call line and set mot to "disabled", but I advise you to leave monitoring turned on after a power outage event.

There is an old saying that criminals always return to the scene of the crime. I don't know if that's always true, but our criminals are very anal-retentive and won't give up easily. So they may call in some favors from another syndicate which has a long history of collusion: your ISP.

I'm not sure if it is feasible for the ISP to disconnect just one DSL or cable modem, but I can imagine they would have some way to block any traffic coming from your modem temporarily. That means that even with backup power, your email alert and attachment will not get through. What to do then?

Although my camera has a proprietary program to save images to a flash drive or hard disk, it's not easily scriptable in a Unix-like environment. To combat this possible attack, then, we must resort to an entirely different setup. Instead of using a WAP, wireless camera, and modem, we will use a digital camera, an old 8x8 WinTV card, and a program called Motion. The OS used is some variation of Linux; in the particular case when I first built this setup, I used RedHat. Motion uses the video4linux interface, so any TV card or digital camera setup that supports video-4linux might work. It's hard to tell with some hardware, but that's why I never throw any hardware away if it still works. Anyway, the setup goes like this: you hook the video-out of the camera into the video-in of the TV card which is sitting in a PCI slot of your desktop computer. You've downloaded Motion from SourceForge.net and have it installed. Here's an excerpt from my motion.conf file:

```
framerate              10
input                  1
norm                   1
auto_brightness        yes
threshold              1000
noise_level            16
night_compensate       yes
lightswitch            yes
daemon                 on
quiet                  yes
execute                /usr/share/alert.sh
target_dir             /home/pics
ffmpeg_cap.new         no
ffmpeg_timelaps        on
thread                 thread1.conf
```

Some things may have changed in the later releases of Motion, so you should read the documentation. I won't go into great detail other to say that threshold controls how sensitively Motion will react to movement, execute means that an alert script is run once motion is detected, and target_dir is where the jpeg images of the detected motion are stored. Right before I log out of my machine and leave my residence, I have a shell script which delays the startup of Motion and runs as a background process:

```
echo "Sleeping for 60 seconds."
sleep 60
echo "Starting motion detector..."
motion
```

That gives me time to get out the door before Motion starts detecting. There are tons of other options that Motion has, such as streaming mpegs, but they are beyond the scope of this article. Returning to our problem of criminals secretly going through our residence, we have to assume that if your ISP is blocking outgoing traffic from your modem, then the miscreants will still have physical access to your system running Motion. That's a problem. If they can reboot your system using some sort of rescue CD, then they might be able to mount your hard drives, search for any jpegs and delete them. What to do?

A while back, I wrote an article for 2600 on loopback encryption on flash drives. You can now read it at `http://uk.geocities.com/➥osin1941`. But I think you get the idea. Using the loopback device, you can create an encrypted filesystem to write the images. Without knowing where to look, any state-supported criminals will not spend that much time looking for your images. And rebooting the machine with a Linux rescue CD won't help them unless they know the password to mount the encrypted file system. Also, there are other open source programs, such as TrueCrypt, out there that let you do the same thing as the loopback encrypted filesystem but on-the-fly. I highly suggest you take the time to acquaint yourself with the various options you have available to you.

It is unlikely that the current state of affairs will ever lead to the repeal of secret warrantless searches. Once criminals get a certain amount of power, they never ever want to relinquish control and, short of an insurgency, it's very hard to break their grasp on our lives. But, armed with the right tools, we can make it harder for them to paint us as terrorists while they themselves excuse their own for similar conduct. And, since equal protection and treatment under the law is now a lie in the United States, it is up to us to start fighting back. I hope this article spawns more articles on leveling the playing field for those of us who don't have powerful friends.

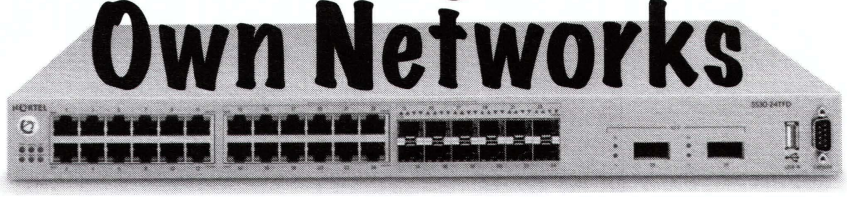
SAVE HOTEL PENN

The home of the HOPE conferences is in danger of being torn down and replaced with a huge office complex. Help us fight to preserve the historic Hotel Pennsylvania, a vital part of New York City since 1919.

Join the discussion at talk.hope.net.

Keep updated at www.savethehotel.org.

Building Your Own Networks



by Casandro

As developments like data retention and censorship become prevalent, it might be wise to build new networks, networks that belong to the users. Back in the BBS days, people operated their own networks like FidoNet over the easily available but unfree telephone network. Today, the Internet is the new unfree network, plagued by companies who want to extort more and more money out of the users. So, it might be a good idea to build your own moderately-sized networks. Even if this won't solve any important problems in the world, it will still be fun.

In this article, I would like to compress all the information needed to do so. This article is a bit Linux-centric, but the ideas should be easy to convert to just about any operating system.

Well what's the obvious thing you need first? Connections. Today we have a lot of possibilities, from IP over carrier pigeon to fast fiber optic connections. The most practical of these are probably WLAN and VPN-Tunnels. The other thing needed is routing. So we need a routing protocol which is simple to use and available to anybody.

Let's start with the connections. Obviously the simplest connection is just an Ethernet cable. Configure the nodes just as usual, and there you go. For larger distances, it might be wise to use WLAN devices in ad-hoc mode. This is probably best explained by an example. Let's assume our wireless device is named wlan0. You can find out its name and settings with the `iwconfig` command. Setting up the device can be a bit tricky. You will need the following commands:

```
iwconfig wlan0 essid "NetworkName"
➥ channel 6 mode ad-hoc commit
ifconfig wlan0 10.111.4.5 netmask
➥ 255.255.255.0
```

The first line sets the wireless device's channel and network. The second command assigns the IP address 10.111.4.5 and netmask 255.255.255.0 to the device. The other wireless devices on the network would have to be in the 10.111.4.x range, with x between 1 and 254. On some cards you will have to first execute an `ifconfig wlan0 up` command to turn on the device. Please choose the IP addresses as randomly as possible to avoid collisions. If you notice that an IP address or range is already taken, use another address.

VPN Tunnels are a bit harder to set up. There are a number of technologies for this, but we'll focus on OpenVPN because it is available for most platforms and easy to set up, at least in shared key mode. First you need to create a key:

```
openvpn --genkey --secret some
➥ file.key
```

This stores the shared key in the file somefile.key. Obviously, you could use any file name for this. This key has to be copied to both ends of the tunnel. OpenVPN then needs a configuration file which tells it what to do. Here's an annotated example. First, the server's configuration file:

```
port 1117  #Be sure to have this UDP
➥ port open to be accessed
➥ from the client
dev tun
# internal server Adr. client address
ifconfig 172.24.13.11 172.24.13.12
# name of your keyfile
secret somefile.key
# periodically send some packets to keep
➥ the connection alive though routers
keepalive 10 120
comp-lzo # compress the data.
```

And the client's:

```
remote nameorip.ofyour.server.org # This
is the IP or ➥domain name of your server
port 1117  # The same as on your server
dev tun
# internal client adr.  server address
ifconfig 172.24.13.12 172.24.13.11
# name of your keyfile
secret somefile.key
# periodically send some packets to keep
➥ the connection alive though routers
keepalive 10 120
comp-lzo # compress the data.
```

As you can see, there are two differences between the server's and the client's configuration files: the client's file has an additional `remote` line, and the `ifconfig` lines have the IP addresses in reverse order. Again, please choose the internal addresses randomly, to avoid collisions. Be sure to always use private addresses.

To start openvpn, just type `openvpn ➥--config your_config_file.conf`. Start openvpn first on your server, then on your client. Most distributions already have init files to start openvpn automatically on boot-up. These often only support one tunnel. If that is enough for you, you can try to use that.

Now, you need to set up the routing. For this we will use OLSR as provided by `olsrd`. This is now probably the most popular daemon for wireless meshed networks. I prefer the 0.5

series as it is considerably more stable than the 0.4 one.

To make it work, you might need to change a few settings in the configuration file,

```
olsrd.conf:
UseHysteresis                  no
LinkQualityLevel               2
```

In the interface section of the file you need to uncomment the line

```
Ip4Broadcast        255.255.255.255
```

and adapt the Interface line to include all your network interfaces. In my case that is:

```
Interface "tun0" "tun1" "tun2"
➥"tun3" "tun4" "tun5" "tun6"
➥"tun7" "tun8" "eth0"
```

Now you can simply start olsrd by typing `olsrd -d 2` on the console. After a short while, the links' status messages should appear. Once you seem to be connected to your peers, you can type `route -n` to get a list of all the routes. Typically, you should get a line for every node in the network.

What if you have computers which cannot run olsrd, for example because they are routers or printers?

For those computers, you can use the host network announcement (HNA) feature. This feature tells the other nodes in the network that your node can reach computers that are not nodes.

In the Hna4 section of `olsrd.conf`, you will find an example of this. You will also have to tell the devices that they can reach the OLSR-managed network via your node. One easy way to do this is to set the devices' default gateway to your computer.

So, what could be accomplished with this? Of course, you could start by connecting your computer to your friends' computers and even to strangers'. Additionally, you could set up a wireless interface. With this, you will be able to offer network access to all members of the network, without having to offer Internet access. If nearby nodes also have wireless devices, they can also form a connection and build a network. Wireless networks were the original application for olsrd. In Berlin, there is such a wireless network consisting of several hundred nodes.

In the dormitory I live in, we have some wireless nodes. Roaming works rather well. You can walk throughout the building and keep your IP address despite being in a different point of the network topology.

As described, this network does not include internet access. If you want to provide it, you have several possibilities. The simplest and most elegant is to set up NAT on your node and use a HNA entry to 0.0.0.0 0.0.0.0 in your `olsrd.conf`. Nodes to which your node is the closest internet gateway will automatically use your connection. There can be several internet gateways; however, be aware that if network topology changes cause you to change your gateway, then stateful protocols like TCP might break.

Another way is to use proxies. For example, I run an anonymity proxy on one of my nodes. This works fairly well if you only want to do web-browsing, as you must manually select your gateway in your web browser.

A good compromise might be to create another VPN tunnel to the internet. This would potentially allow you to have unlimited internet access.

To further obscure the network topology and therefore the position of servers of the network, it might be desirable to install those servers on virtual machines. You could then just migrate the server from one location to another.

I already operate a small network consisting of 3 permanent nodes plus some extra nodes fading in and out. If you want to connect to it, I am willing to give a tunnel to anyone who is willing to give some tunnels to others.

Automation

In order to save you from having to do a lot of monotonous work, I have written a few scripts.

The script `search_ip.sh` first gets a random address from the private address range. If we did not check, there would be a rather high chance of collisions. This is a traditional birthday paradox. Keep in mind that, in addition to this high chance, there is also probability of not recognizing that an IP address is already taken.

When an apparently free IP address is found, the script `write_configuration_files.sh` is executed. This script creates a server and a client configuration file as well as the shared key file and neatly packs them into two zip files, one for the server and one for the client. Please edit the settings at the top of this file to suit them to your needs.

`getkeys.cgi` is a "key dispenser". It gives out a different key file for every request. If you have a very fast computer with a fast connection to the internet, you could use the first script to create a few hundred configuration files and use the cgi-script to get them to your peers.

Be sure to not leave your key files world readable. Not only could they be read by just about anybody on your system, but also OpenVPN will refuse to start.

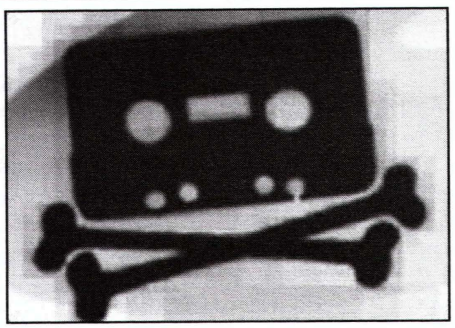
So, let the fun begin.

References:

- *olsrd: http://www.olsr.org*
- *Birthday Paradox: http://en.wikipedia.org ➥/wiki/Birthday_paradox*
- *Large olsrd WLAN-mesh in Berlin (in German): http://www.olsrexperiment.de/*

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

Pirates of the Internet



by black_death
blackdeathx@gmail.com

Yo ho ho and a bottle of caffeinated beverages! We hear about them on the news: evil nerds that make those poor multi-billion dollar record companies and movie studios lose money. But who are pirates really? I'm sure that many people who read this magazine are pirates too, whether you distribute intellectual property or you simply download MP3s. Whether you do or not, this article will be insightful.

I wrote this article because of an article on piracy from the Summer 2004 issue of *2600* that I remember, not because it inspired me but because it was so bad. I was also inspired by how uninformed or just plain ignorant the guys who write for news shows are. Hopefully, my article will shed light on something that few people, not even other hackers, know much about. In this article, I will go into detail about how piracy works. I know that a lot of you guys will know most of the terms but I will define them anyways for the newbies.

Music

This is probably the simplest as well as the most widespread form of piracy; it is also the one you are probably most familiar with. The pirate extracts songs from a CD, which is called ripping them. This can be done either from the official CD on the day of its release or in advance if the pirate works for the record company. Then, the songs are converted to the MP3 audio format, most commonly at a bitrate of 128 kilobits per second, which makes files of relatively low quality. Finally, these new files are put in the "Shared Folder" of the user's peer-to-peer (P2P) program. That's it; the P2P program automatically shares the files with anyone who requests them, so the user doesn't have to worry about anything. Each person who downloads a file also begins sharing it, so even more people can download the file and at faster speeds.

You may have heard on the news about people getting sued by the RIAA, which is an organization representing the four largest American record companies, and some of you might be worried about being sued, but here's my advice: don't worry; they don't have shit on you. That's right: the way these guys "catch" you is by searching for a selected MP3 file of one of the artists they represent and then sending out letters to the households using all of the IP addresses that show up. The same IP is usually shared by several different households even you don't factor in WiFi and the fact that they can't prove who was using the computer. (A robber could've broken in to use your high speed connection because he has dial up, downloaded music, and saved it to their iPod.) If you're still worried, however, download a program called Peer Guardian. It's free and it blocks anti-P2P companies' and government organizations' IPs from connecting to you. Without going on a rant, I'd just like to point out that the record companies have actually made more money since P2P became big: record sales may be down, but internet sales are way up. Also, they barely pay the musicians anything; if it wasn't for ASCAP and BMI giving the artists performance fees for radio play, covers, and the like, most musicians seriously would be dying of hunger.

Movies

If you live in Asia or a large city with a predominantly Asian area (a "Chinatown") in it, then you've probably seen people selling pirated movies. Where do they get them from? Most pirated DVD salesmen download the movies from Torrent sites like Torrentspy and Mininova. This is very easy to do, but the salesmen make money off the chumps who don't know how to do it by selling the movies for anywhere from $1 to $5 each. The movies are usually in VCD format, which is like DVD but lower quality, which can fit on a CD-R, and which can be played on any DVD player. But where those torrents come from is a more interesting story.

Usually the movie is captured by someone sitting in the movie theater with a camera. This was once done very poorly, but now it's usually done with a tripod and an empty theater. These are called "Cam" releases and usually come out the day of the movie's release, but they are also are usually of bad quality. There is also another method called "Telesync" which is basically the same as Cam, except the audio comes through some direct input such as a headphone jack, rather than the camera's microphone. They are also usually better quality than their Cam counterparts. If a movie is very popular, especially among the the white male 14-30 demographic that most often downloads these files, then sometimes a DVD Screener will be released one or two weeks later. These files, sometimes just called "Screeners", are DVD rips made from a DVDs of the movie that are given out only to certain people in the film industry but which then get leaked. Regardless of how the movie was captured, the release group then converts the movie to an XviD file, which is a high quality video format, better than DVD, but which can mostly only be watched on computers and some DVD players, or alternately to VCD format as BIN/CUE disc image files which can be burnt to CD. The files are then distributed as a torrent.

A torrent is a file containing information about which files to download from which BitTorrent

tracker. It basically works the same way as P2P programs, but instead of using Ares or Limewire to search, you use a website. The torrent files are found on torrent websites which either have their own tracker, like . Torrentspy does, or search multiple trackers, like Isohunt does. These are public torrent sites; there are also private torrent sites which you can join by invitation only. On private trackers, the quality of the file you download is usually better and the download usually goes faster, you also have to maintain a certain ratio of how much data you download to how much you upload, and you also have a lower selection of files, unless it's an enormous site such as Oink.

Software, Games, and Other

This is the form of piracy most of you are unfamiliar with because it is the most complicated. Don't get me wrong: it's not complicated; it just seems that way to the average person. Software is usually distributed as a trial version of the software and a crack. A crack is often a modified main executable of the program which bypasses the licensing system, though sometimes all you need a serial number or license key. Games usually come as the full game ripped from the official CDs with the copy protection cracked, plus a serial number or a program that generates serial numbers. Sometimes you'll also get a NoCD program, which is the same as a crack but instead of bypassing the licensing system, it bypasses the system that checks whether the game CD is inserted or not. However, if the game came as CD-ROM disc image files, then you can use a Virtual CD program like Daemon Tools to emulate an actual CD drive instead.

Cracks, key generators, NoCDs, and the like are made by people known as crackers. The crackers use debuggers like OllyDbg and IDA Pro to disassemble the original program's assembly code. They then modify this code with a hex editor such as Hiew or FlexHex. Commercial software programs often try to prevent this by using software protection systems such as Armadillo, ASProtect, or WinLicense, but most crackers can get around these protection systems anyways. There are sites out there that have databases of cracks and serials, but today these sites are so filled with adware and malware they're not even worth visiting unless you really know what you're doing.

Back in the day, warez used to actually be uploaded to one's own FTP or HTTP server or to a hacked server. Now, however, almost everyone uploads to a site called Rapidshare or to one of its many clones like Megaupload. These sites were cool at first but they have wait times of up to a minute before you download can the file you want. This can be bypassed, but a lot of the time it's unsuccessful. Also, because the sites usually limit uploaded files to 100 MB each, warez downloads are usually in 100 MB RAR parts. RAR files are compressed archives similar to ZIP files. The download sites, however, have created something called premium accounts, where you pay monthly for an account that can download an unlimited amount of files without wait times and with prioritized speeds. These premium accounts are often used almost like a currency on warez forums.

Warez forums are internet forums where warez downloads are posted. Most of these downloads, however, are taken from DDL sites, which I'll talk about later. Warez forums have sections for chatting just like other forums; they also have "VIP" sections, which you gain access to by having a certain amount of posts or, more commonly, by donating to the site. These VIP sections supposedly contain rare, high-quality files, but most of the time these sections are disappointing and not worth your money or posting time.

Warez forums used to have very good potential, but now everyone uses DDL sites or torrent sites. This is because all the big Warez forums are currently owned by morons. One example is a forum called WTalk: it started as a very good forum, not because of the admin but because of the powerful and smart people he knew. After a complicated series of events, the administrator banned the people who were the most integral to his forum, and slowly everyone else who was important to the community started to leave or get banned. After a while, the only people left were so childish and stupid ("noobs") that they could relate to the admin. Since everyone with double-digit IQs has left, the only people left to give the administrator advice are the ones as stupid as or stupider than him. They suck up to him, so all his hair-brained ideas have resulted in even lower-quality members and even in more noobs; this is a process I call "Reverse Natural Selection". On top of all, he has also secretly kept a log of his members' passwords, which are supposed to be encrypted, and he's used his members' donations for the site to buy new MacBooks, iPods, and so on. This stupidity and corruption is common among many warez forum admins, though not usually to this degree.

Sorry for my little rant. Anyways, back on topic: DDL sites are websites where the links to downloads are submitted and then displayed as thousand-page lists of software titles. They also, of course, have a search bar. The biggest DDL sites are Katz and PhazeDDL. The sites that submit their links are either actual websites or warez forums, but, either way, they both use Rapidshare most of the time. Also, if you search for a file on a DDL site, most results you get will be redundant: the same Rapidshare link over and over, just with different people getting ad revenue or members.

Conclusion

Warez has come a long way from the "Don't copy that floppy" era, to the rise and fall of Napster and Kazaa, to Torrents, and to people selling something that is supposed to be free. Who knows what the future holds? Maybe one day you'll be able to download physical objects, but what I know for certain is that, right now, warez is at a high point for quantity and low point for quality. It will take something big to fix it. I hope you enjoyed my article and learned something from it. I hope to write for *2600* again.

About me: I have been an active member in the warez community for several years now and sometimes I contribute to the Wikipedia article on warez. I have my own warez forum. It's small but with it, I'm trying to battle the flaws of other warez forums I mentioned earlier in the article. You can visit it at `http://www.kronikfilez.com/`.

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's hard to believe that it's already winter, but the Cascades are covered in snow and ski racks are on almost every car. This is a time of year when a lot of emergencies happen, and the telephone system plays — now more than ever — a vital part in emergency response.

These days, 911 is the virtually universal way throughout the U.S. and Canada to summon the police, fire department, or an ambulance (sometimes all three at once). There is an extremely detailed and rigorous set of standards around how 911 systems and facilities are designed and constructed, and the standard-setting organization is the National Emergency Number Association (NENA).

When you dial 911, the telephone switch invokes an SS7 route that has been specially configured for this purpose. In most cases, your call will be routed over a dedicated trunk to a dedicated 911 switch (although in some areas this is a shared tandem switch — not the recommended configuration but it's better than nothing). The 911 switch looks at your inbound ANI and, based on that, routes you to the appropriate Public Safety Answering Point (PSAP) via a dedicated trunk. At this point — only a couple of seconds after you placed the call — the call answerer will inquire "911, what's your emergency?"

The information available to the 911 call answerer is dependent upon the 911 infrastructure in your area. In most cases, this will be some form of Enhanced 911 (E911), the current standard (most recently updated in 2004). At the network level, E911 consists of a voice circuit (over which you communicate with the call answerer) and a data circuit. The data circuit (which is private, runs a proprietary protocol, and isn't connected to the Internet) is a redundant dedicated connection to an Automatic Location Identification (ALI) database.

Basic 911 provides only a voice connection to the PSAP, with no other identifying data. While call takers have the ability to trace calls, it requires a call to the local phone company which can take up to ten minutes. The limitations of this system are evident when 911 calls are received from people who are disoriented or experiencing medical emergencies and may be unable to answer many questions or even provide the location from which they are calling.

In an effort to solve this problem, the E911 standard was developed. E911-capable PSAPs use Automatic Number Identification (ANI) data to identify callers. Based on this data, your phone number will display on the call answerer's console. The E911 system will also query the ALI database based on your ANI data. In most cases, this database is maintained by Intrado, Incorporated (a private company) and contains CNA (Customer Name/Address) data for nearly everyone in the United States

with a phone — even including unlisted numbers (I bet telemarketers would love to get their hands on this). Newer revisions of E911 include the ability to provide GPS location data for wireless phones, and this data is also obtained via the ALI database. However, these capabilities are fairly new and not yet widely deployed.

While the 911 system is incredibly useful and has saved many lives since it was originally deployed in 1968 (in Haleyville, Alabama and Nome, Alaska of all the random places), it wasn't originally designed to work with newer telecommunications services such as VoIP, wireless phones, and CLECs (Competitive Local Exchange Carriers). These have exploded since the Telecommunications Act of 1996 largely deregulated telephone service, creating both challenges and security vulnerabilities in the 911 system.

VoIP services in particular have illustrated practical vulnerability in the E911 system. Recently, a group of highly unethical phreaks (one of whom was known years ago as "Magnate") was arrested for engaging in an activity called "SWATting." This exploited a little known and multi-tiered loophole in the E911 system.

In case you haven't heard what "SWATting" is, it involves spoofing someone else's ANI when calling a 911 "backdoor" number. Every PSAP in the 911 system has a "backdoor" number by design. These are used by operators to connect you to emergency services if you dial "0" instead of "911" for help. They can also be announced as the emergency contact number via the Emergency Alert System (of "This Is A Test" fame) in the event of a failure in the 911 switch or trunks (this actually happened a few years ago in Seattle). The unethical caller can then describe a violent kidnapping or other situation likely to provoke a SWAT team dispatch by the 911 call taker, who has no idea that the apparent caller is actually the victim of a cruel (and very dangerous) hoax.

Back in the good old days of Ma Bell, nobody could touch the SS7 network except for loyal card carrying CWA union technicians. These days, any idiot with an Asterisk box and a sleazy VoIP provider based in Romania effectively has full SS7 control and the ability to impersonate any ANI they damn well please. This is because with certain VoIP providers, any TNI data that you configure in your VoIP PBX is accepted as gospel by the VoIP carrier, and is sent to the PSTN as both CLID and ANI data. Congress is worried about spoofing Caller ID, but that's small potatoes in my mind — most of the shenanigans around spoofed CLID data are harmless pranks. ANI spoofing, on the other hand — especially when mixed with 911 — is the real problem. If anything damn well ought to be more illegal than it already is, it's this!

And that's the end of my curmudgeoning here from the Central Office, at least for this ski season. Stay in bounds, stop in place if you experience a whiteout, and always keep your mobile phone charged to call the ski patrol!

Links

`http://www.nena.org` – National Emergency Number Association, the standard-setter for 911 systems.

`http://www.qwest.com/wholesale/pcat/911.html` – Qwest 911 interconnection and product offerings for filthy CLECs. This site contains links to many excellent diagrams of Basic 911 and E911 call routing topologies, which incompetent CLEC technicians could never understand.

by WillPC
willpc@hushmail.com

The Beginning of the End

In the beginning, there was the Internet. Everyone happily connected to it, and swapped information freely, without concern for privacy or safety. But soon, this began to change. The fascist regime began to pass legislation, shackling once-free information, and spying on the once-free people. The lightnets were shut down by law enforcement or legal action. Even the decentralized networks, such as BitTorrent trackers, fearing attack, began to become seclusive and private.

The Technology

This new wave of totalitarianism calls for the next generation of file sharing technologies, darknets. Thus far, there have been, roughly speaking, three generations of file sharing technologies, each with a fundamental flaw leading to its demise. The first generation was the centralized and semi-centralized lightnets, such as Napster and even the World Wide Web. However, due to their centralized nature, they were shut down by criminal charges or legal action of some kind. The second generation consisted of decentralized networks, such as gnutella and BitTorrent. Although the decentralized networks are a great improvement over the centralized networks of yesteryear, they, like their ancestors, are flawed. Decentralization was created to combat the legal attacks which destroyed networks like Napster. However, many things were overlooked in their design, namely anonymity and encryption. In the wake of ISP monitoring and RIAA lawsuits, decentralization is not enough. Individuals are being targeted, in order to spread fear.

The Resistance

The third generation of file sharing software is the most important: darknets. A darknet is a private encrypted virtual network for a small group of people. The goal of a darknet is a small, completely encrypted network, completely invisible to anyone who doesn't know about it. Not even your ISP can tell what files are being moved through the heavily encrypted darknet.

Motivations for a Darknet

There are several advantages to darknets. In a small network, with only trusted users, IP farming techniques used by the RIAA and similar organizations are useless. Darknets are heavily encrypted, so they are immune to ISP monitoring tools. Darknets can be "bridged" by users who belong to multiple darknets (see Small World Theory). Becuase darknets are small networks set up by groups who know each other, key distribution becomes a non-issue.

Darknets fix the vulnerabilities suffered by their predecessors, but not without expense. Darknets have one weakness: people. The security of a darknet is based on trust of those using it. Before you invite someone into your group, ask yourself if you really trust that person. Also, set strict rules regarding members inviting new people into your darknet. One lapse of judgment could compromise the security of your darknet. With a tight-knit group of people you trust, and weapons-grade encryption, darknets are the safest, most robust file sharing availible.

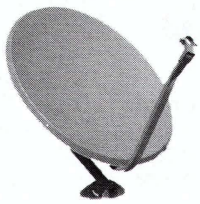
Building a Darknet

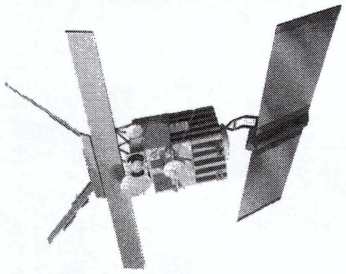
There are a number of ways to build a darknet. Unfortunately, there isn't much software available to do it. Freenet (`freenetproject.org`) and WASTE (`waste.sourceforge.net`) can both be used to create darknets. However, both of these create decentralized darknets. This may seem like a good thing, and in many situations it is. Before deciding on a decentralized network, take into account the size of your network, and how often people keep their computers running. Make sure there is a root node which will always be on, preferably with a static IP.

The second option is a centralized network. Unlike large centralized networks, darknets are not only small and private but also disposable. A larger darknet can be composed of smaller networks, with connections made through shared members, preferably connecting through some sort of proxy in order to protect the identities of the users. A centralized darknet could be constructed in a number of ways, such as an encrypted NFS drive and a secure connection like an ssh tunnel; an encrypted FTP service where each user is given an account which can write to the service; specialized software which uses a hub to cache data (I am writing such software); or a directory, such as a torrent tracker, where all the files are encrypted.

Peace.

Scanning The Skies





by GutBomb

The pursuit of knowledge and understanding of the way things works doesn't need to be limited to computers and telephones. We are being bombarded on a constant basis by microwaves from mobile phone towers, radio transmitters, television broadcast towers, and even from satellites thousands of miles above the earth's equator. These satellites are the focus of this article.

Using a system that only costs about $300, you can explore the exciting world of satellite TV broadcasts from the comfort of your own couch (and the roof of your house from time to time). Sports backhauls, news feeds, syndication uplinks, foreign programming, unbiased news, government propaganda, weather reports, internet access, totally free (free as in beer *and* as in speech) programming, and most importantly, a greater understanding of how the broadcast world works are already being blasted towards you every minute of every day, so why not have some fun?

The Clarke Belt

Television satellites are all lined up along the equator of the Earth. When seen from the Earth's surface, they form an arc across the southern sky known as the Clarke Belt, after science fiction pioneer Arthur C. Clarke. The arc contains over 80 satellites that usually have a name identifying them and a number that corresponds with the longitude meridian they are on. For example, the main Dish Network satellite is known as Echostar 6/8 and it sits in a geosynchronous orbit over the 110 degrees West longitude line. It is often referred to as 110w (read one-ten-west).

Broadcast Bands

There are three commonly used broadcast bands used for satellite television distribution. The Ku-band is the most common method of satellite broadcasting in the country. It is used by both major direct-to-home satellite services (DirecTV and Dish Network) as well as by independent satellite bandwidth providers. Ka-band is a newer technology that has been used for years to distribute satellite internet access and satellite radio but which has recently started making inroads to video distribution. Finally, there is classic C-band, which the major networks use for distributing their channel feeds to other satellite providers and cable companies. C-band requires very large dishes, the smallest of which are nearly 6 feet across. Ku- and Ka-band signals can be pulled in with much smaller dishes, approximately 30 inches across, which are easily mounted on a roof or wall.

Video Standards

Much of the available video up there is now digital. Over the past ten years, most analog video has disappeared on the Ku-band, but you can still find a bit available on C-band. In the case of video distribution, digital does not always mean better. A good standard definition feed on C-band will almost always be better than a digital feed of the same channel because it is the master feed. By the time it reaches your cable or direct-to-home satellite system, it has been encoded digitally, compressed, and bit-starved to the point of looking like a pixelated mess. Analog, however, is a huge bandwidth hog, and prone to interference, so along the way, things progressed more to providing digital feeds. An analog channel takes the same space as up to 20 digital channels, and when satellite providers can provide more bandwidth for channel distribution, they get more money from channel producers. Analog programs are just regular NTSC feeds in North America, and can be picked up by cheap analog receivers.

In the digital realm, the possibilities of what you can find expand greatly. So do the difficulties in initially finding the signal and the expense in getting proper equipment. The main digital standard used for satellite TV in North America is called DVB-S. Most of the world uses DVB variants for their digital television distribution, such as DVB-S for satellite, DVB-T for terrestrial, and DVB-C for cable. In North America we use ATSC for digital terrestrial, and QAM for digital cable.

Equipment

The bare minimum setup you would need to get started is a satellite dish, a TV, and a satellite receiver. The dish is usually a parabolic dish that sits on a mast, with an arm shooting out from the bottom which holds the eye pointing back at the dish. This eye is called a LNB (Low Noise Block). There are a few types of LNBs available. A DirecTV/Dish Network dish contains a circular LNB. Circular refers to the shape of the microwaves being beamed towards it. Circular LNBs pick up spiral shaped beams. These are beamed out at very high power, so the dish itself doesn't need to be very big to pull in the signal. Unfortunately, these LNBs aren't suited to picking up the really cool stuff out there, and the dishes they are attached to are a bit too small, usually between 18 and 20 inches.

For the cool stuff, you will need a linear LNB.

The term linear, like circular, refers to the type of beam it takes in. Linear beams are less powerful and more prone to weather interference, so they require larger dishes. A certain type of linear LNB that can attain frequencies slightly lower than a regular linear LNB is called a universal LNB. The disadvantage to universal LNBs is that not all switches are compatible with them. There are plenty of newer switches, however, that work perfectly, and if you have a single dish system, then you most likely won't need switches anyway.

If you have more than one LNB that you want to connect to your receiver, then you will need to obtain a switch. The best switches to use are called DISEqC switches. (I have no idea how to pronounce this out loud. I say 'diz-e-q-c,' but I am probably wrong.) You can hook four LNBs into the switch, and then just run a single cable down to the receiver.

The LNB I prefer is called the Invacom QPH-031 and you can pick it up for about $80 at any of a number of shops on the internet. It can pick up both circular and universal beams and has two outputs for each. An LNB this fancy is not necessary, however; a cheap $15 universal LNB would be fine for a beginner just getting started.

The dish is an important consideration. A small 18-inch dish won't really do for us, because there are only a few channels available to us legitimately without subscribing to or decrypting an encrypted signal. (This is possible, but not the focus of this article.) Ideally, the best dish to get started with would be 30 inches or larger. I opted for a Fortec FC90P 90cm (36") dish. The dish will come with a mast that you can mount on your roof or on a wall, the reflecting dish, and the LNB arm, but you will have to supply the LNB yourself. This dish will set you back about $100, including shipping.

The receiver is where stuff gets really fun, at least for me. I personally have two receivers. The first is a digital DVB receiver, and then I loop out from it to an old analog receiver. For digital, you have many choices, and unfortunately the market is a bit saturated right now, because these digital receivers can also be used for not-so-legitimate purposes. If you only want to be legit, I recommend the Pansat 2500A receiver. Though it is now discontinued, there are tons of them available on eBay for about $50-$70. It has a very reliable blind-scan feature, which is essential for finding wild feeds.

If you are looking for analog, you may have a much harder time finding a receiver, because they are old and rare. I recently found an analog satellite receiver from the '80s with which you can just dial up the entire map of frequencies, for only $32 shipped. I didn't have a C-band setup so there wasn't very much to find, but the things I did find were pretty interesting: some soccer, college basketball, an outdoor ice hockey game played on a pond, and an FBI training video. Any analog satellite receiver from the Uniden Supra line is highly recommended.

Finally, the last piece of equipment you really won't want to live without is a dish motor. This motor will tilt and pan your dish automatically, so you don't have to go up on the roof every time you want to look at a different satellite. A motor can be found online for about $100. You put your dish on the motor, put the motor on the mast, and point the entire assembly to the satellite closest to true south from your current position. Once you peak your signal there, you can use a feature of the Pansat called USALS that will automatically track the other satellites across the Clarke Belt based on that initial true south positioning. It's amazing to see it in action. My motor of choice is the Stab HH90.

Let's Scan the Skies

Here is where the magic happens. You've got your system all set up, your dish is pointed to true south, you've got your USALS all set up, and you've got your remote in hand. The fun in this is figuring it out, so this won't be a how-to. To point you in the right direction of satellite positions, I recommend `http://www.lyngsat.com`, a listing of satellites around the world and the channels that they contain. Using your receiver, you will tell your dish to point at a specific satellite based on its position (such as 97 degrees West) and blind-scan it. "Blind-scan" will find all channels on the satellite, including full-time channels, data feeds, radio channels, and wildfeeds. Wildfeeds are on-the-spot news reports that are being sent back to the network, which include times when the reporter is "off the air" while their hair is being fixed, they practice their lines, or have candid conversations with the camera crew. You may also find training videos that are broadcast to government agencies and schools around the country. If you're a sports fan, you'll love the sports wildfeeds, which are direct from the stadium broadcasts before they go back to the network. You'll sometimes find these without graphics, commercials, and, more rarely, even without the annoying commentators!

News feeds show up a lot on SBS6 (74w), NASA TV is available on 119w with a circular LNB, and PBS has some network feeds on AMC3 (87w). Aside from wildfeeds, among the other programming available on these satellites (especially 97w) is a ton of foreign programming. You can get an international perspective on news, hit Bollywood movies, sports that aren't normally aired in this region, and just a huge dose of international culture. The real fun is exploring, so I'll leave you to it!

Conclusion

There are tons of things waiting for you to find them up there. Finding something strange and interesting gives me an awesome feeling, and I feel better knowing that I've explored the system enough to gain a greater understanding of the satellite world as a whole. For more information on the topic, check out these great links:
Lyngsat Satellite Index: `http://www.lyngsat.com`
Satelliteguys FTA/MPEG Forum: `http://www.satelliteguys.us/free-air-fta-discussion/`

Shout outs: sxtxixtxcxh, trollsb, my lovely wife Hypher, and JemsTV who helped me out with this article.

Essential Security Tools

by Gr@ve_Rose

Over the course of my career in network security, I have come across a lot of security tools, most of which may already be familiar to people reading this article. Some of you may be a lot more adept with them than I am. With this article, I am hoping to lay groundwork for these tools which people can then build upon. For each tool, I will present where to find it, what it does, how and when to use it, and other tidbits of information which may come in handy.

Name: nmap
Where: `http://insecure.org/nmap/`
What: nmap (Network Mapper) is probably one of the most recognizable names of programs when it comes to network security. Supporting both IPv4 and (some) IPv6, nmap has become a staple for anyone working in network security. It is most commonly known for its port scanning abilities and its ability to customize the scans.
When: nmap comes in very handy for a number of purposes. Vulnerability assessments, penetration tests, testing firewall rules, testing (H/N)IDS functionality, and network audits are the main ones which come to mind off the top of my head, although I'm sure many of you out there have used nmap for other purposes as well.
How: nmap can be used simply as a basic port scanner (`nmap -v -sT $target`). This will perform a full TCP connect scan on most common ports. Or, it can be used for something more complex: `nmap -v -sN -T1 -P0 ➥-p0-65535 -O $target` will perform a NULL (-sN, no flags set) TCP scan, very slowly (-T1), with no ICMP check (-P0) on all 65,536 ports, while attempting to guess the target's operating system based on the results. Using nmap to test your (H/N)IDS signatures and the alerting which goes along with them is a task which will alleviate a lot of headaches when setting up your IDS to test functionality. Using nmap from outside your network and attacking your firewall and any statically NATed hosts will help you audit your current firewall policy and setup. Using some of the advanced options and scan types with nmap will help you hide your hosts from fingerprinting attacks.

Name: amap
Where: `http://www.thc.org/thc-amap/`
What: amap (Application Mapper) is a tool which uses signatures to test application settings against a specific port. If you have ever set up a server, you know that most services can be re-mapped to run on a different port. For instance, editing Apache's "ListenPort" directive will allow you to change which port your webserver is on. If you change this to TCP/22, some scanners may report it as the SSH service. Using amap against this will trigger the HTTP signature and let you know what is really running on the port. amap supports both IPv4 and IPv6 for testing and is very accurate with its results.
When: amap can be used during VAs, RAs, PenTests and system setups or as a trouble-shooting tool.
How: Using amap with the -bqv options is a good start. This will perform banner grabbing and attempt to match against the signature to let you know what is running on the port you have connected to. As a real-life example (sanitized), I had a customer who had rebooted their firewall and incoming TCP port 25 wasn't working. When I telneted to the port, I got an odd banner so I ran amap against it. This is what I got:

```
[root@alice ~]# amap -bqv
➥ 999.888.777.666 25
Using trigger file /usr/local/etc/
➥ appdefs.trig ... loaded 30 triggers
Using response file /usr/local/etc/
➥ appdefs.resp ... loaded 346 responses
Using trigger file /usr/local/etc/
➥ appdefs.rpc ... loaded 450 triggers

amap v5.2 (www.thc.org/thc-amap) started
at 2007-06-24 16:17:34 - MAPPING mode

Total amount of tasks to perform
in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 999.888.777.666:25/tcp (by
trigger http) matches smtp-pix -
banner: 220
****2**********************************
**************************0****0****0
**************2******200***********0*00
amap v5.2 finished at 2007-06-24 16:17:34
```

Noticing that that the banner matches "smtp-pix," I was able to make the modifications to the firewall not to proxy incoming mail. I re-ran amap after and got this:

```
Protocol on 999.888.777.666:25/tcp
(by trigger http) matches smtp -
banner: 220 mail.somedomain.blah Microsoft
ESMTP MAIL Service, Version 6.0.3790.1830
ready at  Sun, 24 Jun 2007 162209 -0400
```

Name: hping
Where: `http://www.hping.org`

What: Using the basics of traceroute, tcptraceroute uses TCP instead of the usual UDP/ICMP combination of traditional traceroute. Some firewalls block normal traceroute traffic but will allow TCP traffic to go through. By using tcptraceroute, you can see the path you're taking on the port you expect to use.

When: If you're troubleshooting and need to find the path a certain packet will take on a multi-homed system or a large network with a lot of dynamic routing, but the intermediary routing devices don't allow regular traceroute, use tcptraceroute instead.

How: Running `tcptraceroute $host ➥$port` will trace the route using TCP SYN packets to the $host on the specified TCP $port. It will first set the TTL to 1 which is expected to die at the first hop and receive an error message from the routing device that the TTL has expired. The program records that IP address as the first hop. It will then increment the TTL to 2 so the packet will make it past the first hop but not the second. This process repeats until either the maximum TTL, which defaults to 30, has been reached or the port is reached, either open or closed. If you don't expect the path to be too long, try using `tcptraceroute -n -q 1 -m 15 $target ➥$port`. The "-n" option, useful at any time, tells tcptraceroute not to perform domain lookups and to give you the IP addresses only. This makes the results quicker as the program doesn't spend time looking up hostnames. Using "-q 1" tells the program to only query the hops once instead of the default three times. Again, this is also useful for almost every time. The last option, "-m 15", specifies the maximum number of hops to use. The default is 30 and it can go as high as 255. Be warned: if you're stuck in an asymmetric routing scenario or are caught in a dynamic routing loop, you may cause some congestion and headaches for the admins.

Name: grass.pl
Where: `http://www.2600.com/code/222/ ➥grass.pl`
What: grass is a Perl program I created (yes, this paragraph is a bit of self-promotion) to help test stateful firewall software and connections tables of the firewalls. It supports both IPv4 and IPv6 and acts as a TCP "door-jam" to create a 3-way handshake. When you're ready to close the connection, a ^C will send the closing 3-way handshake and close the connection.

When: If you have ever worked on a stateful firewall at the low level, you know that they hold connection information usually called a state table or connections table. If the connection table gets full, depending on the firewall software you're using, connections may get dropped. Or, if you try to open a connection on an already established source port, you may have weird effects. grass gives you the ability to choose both the destination and the source port for your traffic.

How: I was working on a customer issue where the firewall appeared to change a SYN packet into an ACK packet. Further troubleshooting found that the device downstream was a wireless router which (for some reason) could only handle 25 connections at a time. When connection 26 came in, it would use the same source port as connection 1 through the wireless router and, when it hit the firewall, the firewall would "help" the packet by changing the flags. I created grass to aid in troubleshooting stateful firewalls or stated connections over TCP.

Name: netcat (nc)
Where: `http://www.vulnwatch.org/netcat/`
What: It's probably easier to say what netcat isn't. Netcat (nc) is hyped as the "Swiss Army Knife" of networking tools and it lives up to that hype. You can use nc for something as simple as creating a TCP connection or you can be more advanced by creating a server-client setup to compress and transfer files between two hosts. You can have nc listening on a server and run a program when you connect to it. The possibilities are almost endless.

How: As much as I want to talk a lot about nc, I think I should keep it short as this article could become a book. nc can be used on it's own or you can put it in your scripts. You can set it up to be a server or even just a listening socket on your TCP stack. I have taken the following example from the nc README file which illustrates a good use for nc:

A typical example of something "rsh" is often used for: on one side,

```
nc -l -p 1234 | uncompress -c | tar xvfp -
```

and then on the other side

```
tar cfp - /some/dir | compress -c | nc ➥-w 3 othermachine 1234
```

will transfer the contents of a directory from one machine to another, without having to worry about .rhosts files, user accounts, or inetd configurations at either end.

As you can see, using nc in addition to what you normally do can make life a lot easier. You can build a basic automated file transfer program between two machines with a little knowledge of scripting, some nc and a cron job. Netcat is worth sitting down with a pot of coffee and playing around with.

Name: ike-scan
Where: `http://www.nta-monitor.com/ ➥tools/ike-scan/`
What: ike-scan has a name which is a bit misleading as it doesn't rely on ISAKMP only; it does IPSec scanning as well. If you are performing a VA, SA or PenTest against a VPN-capable machine, ike-scan is a must.

How: Using ike-scan may require a bit of reading on their wiki site to glean a good amount of usage information. By itself, ike-scan will go and attempt to gain as much information about the VPN target as it can: Is it using Aggressive Mode? What encryption and hashing methods

are supported? What sort of authentication is being done? These are just a few questions which ike-scan will attempt to answer for you. In addition to performing basic enumeration, ike-scan can be used to negotiate full VPN connectivity, though this may not be for everyone to try. I have found that ike-scan is very helpful when troubleshooting VPN connections, especially when you don't control the remote end. Some VPN error messages from specific vendors can be rather cryptic (No Valid SA - Ye olde generic Checkpoint Error Message) and ike-scan helps give you good information in determining where the problem may lie. Using ike-scan in your VA, SA and PenTest work is also very helpful.

There are a *lot* more security tools out there which I haven't mentioned, including among others hunt, a session hijacker; thc-hydra, a password auditor; and thc-ipv6, an IPv6 attack toolkit. All of these, and others I haven't touched upon, could be put together to have a book written about them. I just wanted to draw some attention to the ones which I use on a regular basis and find most helpful in my day-to-day security work. In other words, if I didn't mention $your_favorite_program in this article, I'm not trying to slight you, the tool's authors, or its importance. I hope you find this article useful and begin to explore the uses of these and other programs. Once you become accustomed to how they work, you will find yourself using them in all sorts of scenarios in which you may not have thought of using them but in which they will help you out immensely.

Decoding Experts-Exchange.com

by Phatbot
chunkylover37@gmail.com

At work this week, I was trying to resolve a particularly pernicious bug, so I Googled for the error message and came up with this:

```
http://www.experts-exchange.com/
➥Programming/Misc/Q_20914397.html
```

Experts-exchange — hmm, that's awfully close to ExpertSexChange.com, another of my favorite websites! Er, not really.

Like many such sites, they would like your money before showing you the solutions to the questions posted. But unlike other sites, Experts-Exchange actually does show you the solutions, just in a grayed-out box that's hard to read.

When I've come across this site in the past, I just viewed the HTML source, and there you could read the answers in plain text, thus saving you their $20 yearly fee. But this time, the answers looked like this:

"Vg'f abg nf hahfhny nf lbh znxr vg fbhaq..."

Not terribly helpful, but I guessed that they were using a simple substitution algorithm to encrypt the text. I quickly fired up a text editor, copied the encrypted text to a file called `experts-exchange.txt`, and wrote this Perl script:

```
open(IN,'experts-exchange.txt');
my $text = join('',<IN>);
close IN;
$text =~ tr{VvGgFf}{IiTtSs};
print $text;
```

I'm using the "`tr`" (transliteration) operator to change each V in the text into an I, and so on. I just guessed that the string "Vg'f" was supposed to be the word "It's."

The result looked promising, so I just kept making guesses. Ultimately my decoding looked something like this:

```
$text =~ tr{AaBbCcEeFfGgHhIiJjLlM
➥mNnOoPpQqRrSsTtUuVvWwYyZz}
  {NnOoPpRrSsTtUuVvWwYyZzAaBbCcDdE
➥eFfGgHhIiJjLlMm};
```

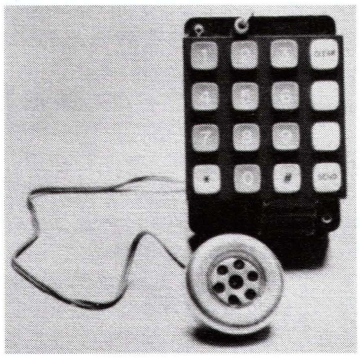
With everything in alphabetical order like that, it's pretty easy to see that the text was just rot13-encoded. So, this simplified Perl script took care of decoding the whole thing:

```
open(IN,'experts-exchange.txt');
my $text = join('',<IN>);
close IN;
$text =~ tr{A-Z}{N-ZA-M};
$text =~ tr{a-z}{n-za-m};
print $text;
```

Now, in my case, the decoded text didn't get me any further toward solving my original problem than the encoded text, but it was a fun diversion. Your mileage may vary.

Editorial Note: As of press time, we have been notified that Experts-Exchange has recently changed its website so that the ROT-13 decoding algorithm described here will no longer work. We hope that our readers will nonetheless find the article instructive.

An Introduction to Beige Boxing



By Erik Paulsen

I'm going to take a few moments to take things back to the basics: I'm going to teach you beige boxing. Beige boxes go back to the origins of hacking, when accessing other people's phone lines helped you remain undetected. Using hijacked phone lines helped conceal crimes that were committed through modem connections.

Beige boxing is a science; employing it in practical situations is an art. Beige boxing will permit you to connect a phone, laptop, or Palm Pilot to a telephone landline. Whether you are learning by tapping into your own phone line, or someone else's, there are only a couple of basic parts and tools you will need to get started. Once you've learned to beige box, you can learn more about more advanced topics including DTMF tones, red boxing, social engineering, wardialing, and wiretapping.

So, let's start with something basic. As I go through the following examples, I expect that you are already familiar with the following things: you know what a phone is, you know how to dial a phone number, you know what a modular phone jack is. If you're using a modem, I also expect that you know how to dial with that modem and how to do whatever else you want to over the phone line once connected.

Also, it helps to have common sense when doing anything clandestine. If you plan to do anything illegal, or anything that you think might be illegal, check your local laws and try not to break them. Beige boxing offenses, in the eyes of the law, usually involve trespassing, theft of services. Connecting to the internet by beige boxing may be considered a federal offense, since the illegal phone connection will more than likely cross state lines.

The Most Simple Device You Have Ever Made: The Beige Box

A "beige box," or a homemade "lineman's handset," is a simple telephone cord modification. It is called a beige box because the first version ever made supposedly used a beige phone. I'm sure you can learn more about this if you look for a description on the Hacker's Lexicon.

Construction is simple. You'll need a few parts: one modular phone cord, which will be mutilated; two solder-type or screw-type alligator clips, preferably insulated; a soldering iron or screwdriver (accordingly); and something to cut and splice the phone cord, typically a wire cutter which will double as a wire splicer. Finally, you will need a phone, and you won't be doing anything to it.

So choose an appropriate phone. Obviously, the phone you will be using to Beige Box will need portability! If you can't use it with one hand or less, don't bother with it. A decent hands-free telephone is ideal.

First, cut the phone cord as close to one of the ends as possible, so you have a phone cord with a modular jack at only one end. Next, you will want to splice the same end of the cord that was just cut. This will expose the two (sometimes four) color-coated wires inside the cord. We will only be dealing with the red and green wires, so if you also have yellow and black wires, you can carefully cut them off.

The object here is that you want to connect your two alligator clips to the two separate wires inside of the phone cord. I would say you will only need to expose the last two inches or so of the outer plastic cover. This will leave you with two wires, one red, and one green, sticking out two inches from the end of the cord. Then, strip a little of the plastic jacket off the red and the green wires, so you have enough bare wire to connect the clips.

Finally, attach the alligator clips, one to each stripped wire. Now, it doesn't actually look like a box, but you can plug it into your one-piece phone. Construction is now finished, and you have just made a beige box.

I'm sure you're now wondering what you can do with the box you've just built. To test it out, look for your home phone line's junction box. This is where your phone line comes into the house and where it is wired to your home's telephone wires. It will typically be found on the outside of the house but may be in a garage or possibly by your house's fusebox. I have seen junction boxes located in many places, from apartment building laundry rooms to hotel utility closets, but I'm sure your search will quickly succeed.

Once you have found your junction box, open it up. If it has a lock on it, use your judgment and your common sense. If you keep reading, I'll assume you've got it open. These are customer boxes, so the person who pays for the phone will own the equipment.

What we are aiming for is a bridge-type connection, allowing your phone to access the landline. So, you will want to connect your alligator clips. If you're smart, you won't reach your hand into the junction box and fiddle around, as there is electrical current flowing through the wires. It will typically be only 20 volts of direct

current, but if the phone happens to ring, you'll get a nice "wake-up call," as ringing voltage is around 100 volts of alternating current.

Respecting the electricity inside of the box and observing reasonable safety measures, attach the alligator clips accordingly: red to red, green to green. You may notice that green, red, black, and yellow wires are connected to your four terminals. You will be attaching your alligator clips to the red- and green-wired terminals.

Hopefully your junction box is wired this simply. If this is not the case, remember the rule: right red ring, left green tip. Or, more simply: right red. Some boxes are wired this way instead of using colored wires. So attach your red wire with the right terminal (which is usually a screw) and your green wire to the left terminal (also a screw). Correctly attached, with a phone plugged in, you should get a dial tone. This means success.

You can connect your beige box to any phone line which you can access. You can expand this to network junction boxes, which are the ugly green boxes located in residential areas, and to buried phone cable lines if you can match the correct wires together. You may be surprised to see how many phone lines are grouped together in one location.

Now what you do with it is up to your imagination, and is only limited by the laws of electricity. An FM transmitter can be attached to a phone line. So can audio input and output connectors and a multitude of other devices and applications. Beige boxing simply taps into a phone line. After that, there's not much of a limit.

A note to those who are unfamiliar with technological tampering: this device is not meant to harass the AT&T operator, enemies, or ex-girlfriends. It is not meant as a tool to stalk someone or to listen to private phone calls. It is not intended to do any damage, physical or emotional. It is a tool for learning about the physical aspects of and possibilities of this technology.

Glossary of Terms

Dual-Tone Multi-Frequency (DTMF) Tones: The tones emitted by a touch-tone telephone or a device modified to emit such tones. As well as dialing phone numbers, they are also used to control telephone equipment, including electronic switching equipment and payphones.

Red Box: A modified DTMF tone dialer that generates the tones which tell a payphone that a quarter, dime, or nickel has been deposited. Since its discovery, the possibility of red boxing has been widely eliminated by telephone company countermeasures.

Social Engineering: Acquiring information through manipulative social interaction.

Wardialing: The act of dialing phone numbers in a sequence to search for telephone numbers with interesting properties or for phone lines connected to modems.

Wiretapping: Recording or transmitting the conversation taking place over a phone line, in order to listen to conversations and gather information.

Lineman's Handset: A device used by telephone company repairmen to connect to a phone line for testing purposes. A professional and feature-enhanced version of the beige box.

by Mercereau (aka dohboy)
http://www.dohboy.com/

When I first installed my new flash drive, a Sandisk Cruzer Micro 2GB, I found the application that was autoloaded, Launchpad, to be a bit clunky and cumbersome. Of course, I was using an older machine at work which was at end of life cycle a year prior. The graphical features were nice, and the concept was fantastic; to me, it seemed to be an attempt at a portable operating system in that you could transport all of your applications, which would remain on the drive. Even so, the removal of the additional drive became necessary, as my position required hopping from machine to machine. Waiting for the drive to install each time meant wasting time.

While this article is not a tutorial about U3 removal, you can go to `http://www.u3.com/uninstall/` to remove the U3 if you want. To my knowledge, this will permanently remove the U3 with no way of reinstalling it at a later date. Doing this will make the rest of this article irrelevant. Please note: in no way am I responsible for you breaking your drive as a result of the procedures below.

Basic Information

There are some basic things you should know about the U3 Smart Drive. The U3 comes pre-partitioned; most of the device is a FAT partition with a hidden SYSTEM file. SYSTEM is where all of your programs are stored. The last four to six megabytes or so are allocated to an ISO-9960 partition that emulates a CD-ROM drive. Within the CD-ROM partition, there is an autorun.inf which kicks off the installation of the Launchpad. The Launchpad is the main program for management of the applications installed on the drive, as well as for file management and data encryption. The U3 runs on (almost)

any PC running Windows 200 SP4+, XP, or Vista.

Some of the U3's features are portability and the fact that you don't need admin rights to install new software. Some of the negative aspects are the need for two separate drive letters, trace files that are sometimes left on the host PC after improper removal, and the wait time needed for the initial installation of the U3 (in some cases, up to 3 minutes from personal experience).

The CD-ROM partition on the SanDisk Micro cannot be written to like a normal CD. There is some amount of reverse engineering involved; however, if you can run MagicISO, by the end of this short article, you should be able to re-write your U3. I began looking for ways to remove the drive and found various other tools that I could use.

Tools Needed

First, you will need to download LPInstaller.exe. LPInstaller is required to write to the CD-ROM partition. You can download this from `http://www.sandisk.com/Retail/Default.aspx?CatID=1411` or you can visit my site at `http://www.dohboy.net`. Second, you will need to write an ISO that the LPInstaller will use to 'burn' to the U3's CD-ROM. You can do this with the help of MagicISO (`http://www.magiciso.com/`). Even if you do not have the full version, the trial version allows you to create an image smaller than 400MB. That's it.

Re-Writing the U3

Some have tried to rewrite the U3 by craftily using Linux; some have attempted this using some fancy host file modification to mimic SanDisk's web server, but all you really have to do is save the image you have created as "`cruzer-autorun.iso`" in the same directory as the LPInstaller. Once the LPInstaller is run, it will grab the "`cruzer-autorun.iso`" and use it, since it believes this file has already been downloaded. If the file is not in that location and there is an internet connection available, LPInstaller will go to the SanDisk website and download the most up to date version of the Launchpad. You can see what Launchpad tries to connect to using ethereal. There is a limitation to the size of the image: 6.2MB. I have tried larger but only got errors.

Remember, the image must be named `cruzer-autorun.iso` and be in the same directory as LPInstaller. LPInstaller will write the .iso file to the flash drive's CD-ROM partition. I probably don't have to mention it, but make sure the U3 is actually plugged into the computer before running LPInstaller. In my line of work, I am used to working with the lowest common denominator.

Tips

autorun.inf

```
[AutoRun]
open = "program.exe"
icon = .\dohboy.ico,0
```

Save the above information, replacing *program.exe* with any globally-executable application on the host machine or any application on the U3 partition. For instance, if you have an application on the U3 called haxor.exe in the root directory of the CD-ROM partition, you would reference it using `.\haxor.exe`. Autorun.inf must be in the image's root directory, just like with any autorun file.

Visual Basic Script, though it is slower and uglier, is my code of choice. These files are easy to create and can be launched as long as wscript or cscript is on the host machine. If they are not, either can also be written to your partition; you are only losing 112KB by doing so.

Implementations

Thus far, I have written various scripts and applications for the U3 which make my job easier and my life more fun. One such script will allow me to track my U3 if it is lost or stolen. This was done using the `getInfo.vbs` script available in the 2600 code repository or on my website at `http://www.dohboy.net`. This script will send me an email with the login, domain, local IP address, public IP address, registered owner, and other information of anyone using the lost or stolen U3. This is only if the user is currently connected to the internet and has no limitation on their ability to connect to my SMTP server. I plan on developing a free service that would allow a user to track their U3 in the event that it was lost or stolen via my website. It is a work in progress.

It might also be possible to write scripts that would allow you to poll the system for information and write it to a file located on the FAT partition. How is that possible if the drive letter could be different from machine to machine? Make the script search for a file from all possible drives and append information when found. Various other scripts like this can be found on my site as well.

Another implementation of mine was a keylogger. I used C++ to create an invisible application called squid.exe (I might post this on my website) that logged keys. The way it worked was to load upon launch and log keys. Once the thumbdrive was plugged back into the machine, squid would know that the drive was plugged in again, and would search for a specific file in the root of the FAT partition. After the file was written, squid would exit with garbage cleanup. No files on the host computer would be created.

For fun, rewrite the `autorun.inf` to open a shutdown sequence. (for example: "`shutdown -r -t 00`")

Conclusion

While some of these implementations are fairly tame, there are potentially far more dangerous scripts and programs that can be written. My squid was a fairly slow application since I only wrote it to test what I could do. While it performed as I had planned, it could have been optimized to be quite a bit faster and run without using as many system resources.

While this article focused mainly on the SanDisk because of its vulnerability with LPInstaller, there is a possibility the partition on any U3 could be rewritten. More information on hardware, such as the HDK, might be obtained by emailing `licensing@u3.org`. Have fun with your U3 and try not to get in trouble using it.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

Exploring AT&T's Wireless Account Security

by satevia

I'm writing this article to inform the readers about the potential insecurities of their wireless phone service. I used to work for Cingular, so most of this information will apply directly to their service. That's not to say that things are any different with other providers, but I have no specific internal experience with them. I'd also like to remind the readers that this information should be used as a guide to further secure access to your own wireless phone service account and not to breach the security of others.

Cingular has changed its name to AT&T since I originally started writing this article. That's the only thing that has changed, so this does not make this article useless and does not mean that your account is any more secure.

Wireless carriers store a scary amount of personal information about each of their customers. Even scarier, every support representative has access to this information simply by plugging in any bit of identifying information about you or your account. Among other options, this can be your name, date of birth, social security number, address, home phone number, or cell phone number. Just about anything specifically relating to you can be used to pull up even more information about you. Even worse, much or all of this information can be used by anyone that calls into the support department to change information on your account, add services, or remove services. That list goes on and on too.

By default when you call into AT&T customer care and reach an operator, generally after hours of holding, you're asked to confirm your wireless number. This generally comes up automatically on the screen, which is called the "screen pop" internally. Along with that is the first screen that the representative must click through after they've confirmed your access to the account. They're supposed to click which of the security measures was used to verify your identity. Representatives are told to ask for the last four digits of the social security number, though with enough complaining you can generally get them to give you access to the account by providing the billing address on file. Great!

After the representative has clicked through, confirming that your identity has been verified, a log entry is placed on the account showing which representative accessed the account and when. This can be easily bypassed by clicking the "cancel" button located on the screen pop window, or by accessing the internal database, Telegence, directly and not through the initial verification system, the name of which escapes me. Many representatives do this if they're lazy. Telegence is where all of the goodness is. The search feature allows the agent to pull up accounts using any of the identifying information mentioned above. You can generally pick out a lazy representative as one that asks you to confirm your phone number if you entered it when calling in or if you pressed 1 to confirm the caller ID.

A quick note about notes (ha!): even though representatives may make notes on accounts and even though the system still makes notes automatically for just about every action taken, they don't really mean anything good for you. Generally notes are a place where representatives explain to other representatives that may field your call later whether or not they should believe what you say or go out of their way to help you. Did you get angry with a previous representative or sound frustrated? Yeah, that'll probably follow you for the life of your account. The life of an AT&T representative is not a fun one and each day really drags along. You hear the same thing nearly every call and get yelled at nearly every call. The only way for representatives to get back at you without getting fired is to make your notes sound like you were as uncooperative as possible. And they will.

In addition to information stored electronically, AT&T call centers always have pages and notepads filled with identifying information laying around. Representatives are trained to write down specific information gathered when on a call, in order to prevent having to ask a customer again. This includes credit card numbers used for payments over the phone. Thankfully, security at the call centers themselves is fairly good (seriously), but visitors are allowed to be escorted throughout the building by any employee. Technically, guests are not allowed in the work area, but this rule is largely ignored. Badges must be displayed at all times and I've actually had security question me when mine had simply flipped around. Kudos for that. Unfortunately, kindness is what breaks this down. It's quite easy to gain access to a call center itself simply by entering during the morning rush, when everyone else shows up for work. Despite the extensive video-based training advising that employees are to watch out for "tailing" through the entrance, it's human nature to hold the door open for your fellow representative as they come

to the door after you. Everyone does this. This, coupled with sensitive customer information available on just about every desk, leads to the potential for disaster.

Let's assume physical access, though, is hard to get, but the fact that your information is available to all representatives opens a new door for anyone to get or change this information. A number of news articles have recently been published which show how easy it is to buy information about anyone's social security number or address. This would allow the defeat of both security measures in place by AT&T. Even if you don't have this information or don't want to pay for it, losing your phone is a great start to giving up control of your phone service.

Many people don't think to call in and have their phone suspended immediately, so there's a great chance that dialing 611 (for customer service) on a found phone will be about the most effort needed to gain access to an account. The automated phone prompt speaks back the phone number (write this down) that's calling, saving you from having to call yourself to find the phone number and placing your phone number on that customer's call log. This answers question #1 by the representative, "What's the wireless number you're calling in reference to?" Rarely, some representatives will ask for the full name of the person that's calling. It's for logging purposes only and gets entered into the notes of the wireless number's account; access is not restricted on a per-name basis. If this happens, you can generally give any name you'd like and still proceed through the verification process. Next, you'll go through the authentication process described above. Remember that knowing the victim's address is usually enough to get through. Once verified, the account is yours. You're free to add or remove services, change contact information, change wireless numbers, request that call records be mailed to an address, or anything else you like. Everything can be done over the phone once you're "verified".

You might be wondering exactly how you'd get someone's address, especially if you just found a phone lying around. That part is actually surprisingly easy. Heading into an independent AT&T dealer with the phone number for the account is enough. Remember to call 611 and listen for the phone number to be repeated, so you don't have to have to call any of your phones and have the number logged into their call log. If you did call your own number, the logs would be kept not just on the phone, but also on the computers used by AT&T to monitor minutes, usage, and on the list mailed to customers each month as part of their bill.

You can generally distinguish a dealer from a corporate store by the actual name of the company running the store listed on or around the Cingular/AT&T logo on the door or window. Otherwise, you can always ask a representative as they're supposed to truthfully answer the question.

Dealers are generally underpaid representatives for a third-party company with no relation to AT&T other than their reseller status. They usually care about nothing more than getting you to upgrade your text message package or adding internet access as they make a large chunk of commission off of "extras." With that comes a lack of care for the security of accounts. I guess that they assume that just knowing the phone number on an account and that the service is from AT&T is authentication enough for them and that this information alone should provide access to the account. Next, asking to verify the billing address on file for the account should be enough to get them to tell you. Writing this down would be a bad idea, so try to remember it. I'm sure you could also get them to give you the social security number by stating you tried to call and the numbers you gave were denied, so they told you to come in to a store and have it changed.

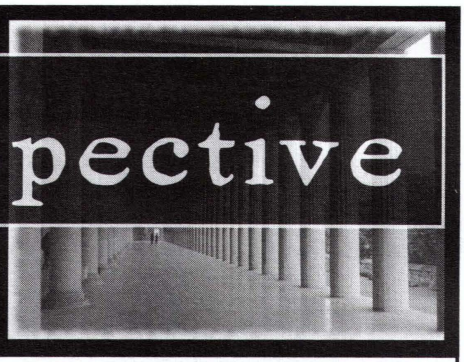
Then all you need to do is call customer care again, address in brain, and you've successfully penetrated the deep defenses of AT&T.

A (semi-)great way to prevent all of this from happening is to place a password on the account. This password supersedes any other form of authentication at least, it's supposed to. Provided the representative over the phone realizes that there is a password on the account, the account can not be accessed without knowing this password. Unfortunately the only way a representative knows that a password is on an account is by the small, unbolded red text that appears as one of the authentication methods listed when you first call in. Unfortunately, the system doesn't require that this method be used, and representatives are more in touch with their routine and are to preoccupied with the need to handle as many calls as possible in one day (call stats matter, you know) even to notice it most of the time. Passworded accounts are commonly accessed without the password over the phone due to the inattentive representative on the line. Scary! It's the only access control that you can place on your account, though.

Even if you do all that you can to protect your account, you can't compensate for poor corporate teaching. Encouraging representatives to write down personal information for customers they deal with is bad practice. I'd much rather have to repeat my information than have it lying around on someone's desk for the prying eye or unwanted visitor to see. The contracted cleaning crews that come in nightly probably don't care about your privacy either, and full credit card numbers with names and addresses are readily available for their viewing as they clean, unwatched, each night.

I hope that this article has proved useful to everyone with a cell phone. They're not quite as secure and private as everyone imagines and expects them to be. With better training, better pay, and stricter hiring standards, AT&T could pretty easily change this around and greatly increase the protection they provide for their customers' personal information.

Hacker Perspective



Rop Gonggrijp

My most recent confrontation with what it means to be a hacker started in March of 2006, after I went to vote for the local council of Amsterdam. At the polling station, I had to use a brand new electronic voting machine that the city was renting from a company called Sdu. In fact, Amsterdam had contracted the entire election as a turnkey service. Sdu was even training the poll-workers. This "voting machine" was in fact a computer with a touch screen running Windows. To make matters worse, inside each computer was a GPRS wireless modem that sent the election results to Sdu, which in turn told the city. I had not been blind to the problems of electronic voting before, but now I was having my face rubbed in it. And it hurt.

Perhaps I should quickly introduce myself. My name is Rop Gonggrijp and I'm a Dutch national who lives in Amsterdam, The Netherlands. Some of you will know me as I have been mentioned in this magazine as well as been a regular guest on *Off The Hook* for almost as long as the show has existed. I'm one of the main organizers for those Dutch hacker events like Galactic Hacker Party, Hacking at the End of the Universe, HAL 2001, etc. Between 1989 and 1993 I published *Hack-Tic*, a magazine not unlike *2600* except that it was written in Dutch. During the late *Hack-Tic* years I co-founded XS4ALL, which still is one of the larger ISPs in The Netherlands.

I guess I became part of the hacker community sometime during the early 1980s while playing with my father's 300 baud acoustic modem, although arguably I was hacking before - when I was soldering FM transmitters together with a friend at age 12. But after reading Steven Levy's book *Hackers, Heroes of the Computer Revolution*, I knew what I was and that I was to be part of a global community, even if I could only knew a few other hackers around me. Imagine my relief when I went to Hamburg for the 1988 Chaos Communication Congress to find a few hundred other hackers. After that I was hooked, and by 1989 I was one of the organizers of the first European hacker event: the Galactic Hacker Party. Long and formative years of exploration, mayhem, and mischief followed, during which, among many other things, we found and shared many new and interesting ways of making free phone calls. And when we got our hands on the keys to the nuclear bunkers that existed underneath some subway stations in Amsterdam, we promptly organized tours there for all our friends and their friends. But even behind the greatest mischief was the motivation to educate, to sharpen the minds of fellow hackers and

of the population at large.

XS4ALL, the Internet provider, was much more a political statement than anything else. The Internet back then would never make any money: way too difficult and freaky for the general population. I left XS4ALL in 1997 and started a computer security consultancy, and then after that a company that builds voice encrypting mobile phones. But I kept going to hacker events and co-organizing our own event every four years.

Fast forward to 2006 and the local elections. I was angry because I felt my election had been stolen. There was no way to observe a count, one just had to believe that this wireless-equipped black-box Windows machine was counting honestly. I knew a little bit too much about the risks associated with computer technology to go along with that. I wasn't the only one who was angry. My longtime friend Barry came home from that March 2006 election with the exact same story that I had come home with: trying to reason with poll-workers who clearly felt that only the medically paranoid would distrust such a wonderful shiny box. When we met later that day, we vowed to not only get mad but to do something about it.

But that wasn't going to be all that easy. By the time Amsterdam had gotten electronic voting, it was pretty late in the game: Amsterdam, with a population of approximately 750,000, was the last city in The Netherlands (with a population of around 16.5 million) to get electronic voting. Some cities were renting the same system that Amsterdam now had, but the vast majority was using an older system made by a company called Nedap. While I studied the legal requirements for electronic voting, I became even more convinced that all of these "machines" (that were all in fact computers) needed to go if we were to have transparent and verifiable elections. The regulations treated these systems as if they were indeed mere "machines." They worried about the amounts of humidity and vibration they could withstand and they made sure nobody would get shocked from touching one. Computer security wasn't even mentioned. But the biggest problem wasn't the lack of security, it was the lack of transparency. We got together a small group of like-minded people and started planning a campaign.

There had been previous attempts to raise the question of trustworthiness in relation to voting machines, but the Ministry of the Interior was used to painting the opponents of electronic voting as technophobe Luddites. Given that half of our group consisted of hi-tech-loving hackers, this was an approach that wasn't going to work this time. During the next year and a half we managed to get the attention of the media. We claimed that the Nedap "machines" were computers and not "dedicated hardware" (as the manufacturer claimed) and that they could just as easily be taught to play chess or lie about election results. The person selling these computers in the Netherlands wrote wonderful long rants on his website, and in reaction to our claim he said he did not believe his "machines"

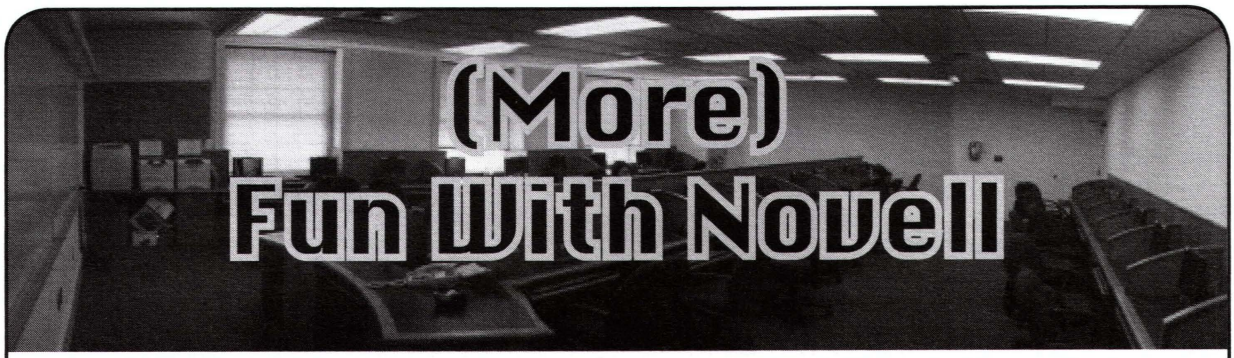
could play chess.

So we caused a true media frenzy when we got hold of a Nedap voting computer and made it play chess. (We also made it lie about election results.) There was a debate in Parliament, during which the responsible minister promised to appoint two committees. That next election, an international election observation mission studied the problems with electronic voting in the country which until then had always been the example country for uncontroversial e-Voting. In their report, they advised that these types of voting computers "should be phased out" and the two committees also wrote very harsh reports about how these "machines" came about and how they should not be used in the future. A lot more happened. We threatened to take the government to court on several occasions, and we even won a case in which the Nedap approval was nullified. But by then the ministry had already decided to throw in the towel, retracting the legislation that allowed electronic voting. The next elections in The Netherlands will be held using pencils and paper (which is really quite OK since over here we've only got one race per election, so counting by hand isn't all that hard).

One of the things that struck me about this campaign was that in order to win, we've needed almost every hacker skill imaginable. Imagine all the stuff you can learn from this magazine, or from going to (or helping organize) a hacker convention. From general skills such as dealing with the media or writing press releases to social engineering (getting hold of the system in order to experiment with it), lockpicking (showing that the mechanical locks were bogus as the same one Euro key was used all over the country), reverse engineering (modifying their 68000 code without access to source), and system administration (website).

Having published a hacker magazine and done the ISP, I was no stranger to conflict. At XS4ALL we had had serious issues with the infamous "church" of Scientology as well as with the German government. Also, the international contacts I got from growing up in the hacker community paid off: the hack was very much a Dutch-German project, and we're still working together tightly to also get rid of these same "machines" in Germany. At certain moments I had the funny feeling that somehow this was the project that I had been in training for all these years.

So I guess what I'm saying is that if you are a hacker, if you're going to hacker conventions, if you like figuring stuff out or if you are building your own projects.... Please realize that, possibly by accident, you may also possess some truly powerful skills that can help bring about political change, and that these skills will become more and more important as technology becomes a bigger part of ever more political debates. So if you don't like the news, go out and make some of your own!



(More) Fun With Novell

by Cronicl3
cronicl3@gmail.com

I've received a lot of e-mails from people in reference to my article in 23:4, and I figured I'd write up this addendum to it addressing a lot of the common issues and discussing some further exploits. The most common issue I was asked about is the "software conflict" with Norton AntiVirus. When you put the pwdump files on a flash drive or e-mail them to yourself, Norton eats up the files almost immediately. If you can access msconfig and regedit, then you can just turn off the auto-protect and so it's no longer an issue; however, Norton does have some defense against this, and most users are locked out of those utilities. An even simpler and more obvious solution is to just uninstall Norton altogether. Most institutions use Norton AV Corporate Edition, which you cannot uninstall it without a password. Fortunately, incompetent admins such as mine don't change the default password which is "symantec". Another issue commonly encountered was lack of access to the command prompt. The easiest way to get there is to open up IE and put `C:\Windows\System32\` in the address bar. Then, CMD is right there. However, if this is not an option, you can always put the pwdump2 executable and .dll on a flash drive and write a simple little runme.bat batch file with the following code:

```
pwdump2 > output.txt
```

This will capture the hashes output by pwdump to a text file called output.txt, so you can just open up your flash drive, double-click your batch file, and not even have to worry about getting manual command prompt access.

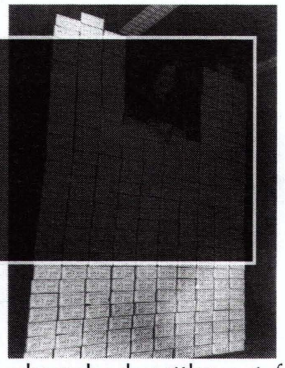
Over the past several months, I've also furthered the depth of my exploits and explored them to the greater of their potential. The PsTools suite, previously owned by sysinternals and recently bought out by Micro$oft, has some great tools. For example, psshutdown and psexec are awesome little programs that you can use to remotely shutdown machines and execute programs. You can have great fun with this during presentations. Here's a quick anecdote for you: there was this new teacher that everyone hated because he didn't know any of the material he was supposed to be teaching and acted as more of a police officer in the class rather than a teacher. He would constantly kick kids out or give them detentions for ridiculous things like checking the weather or their e-mail; one kid even got his computer privileges suspended because he was caught downloading Firefox. Forgive the kid for not wanting to use Internet Explorer 6, the browser that makes any security professional quake with fear. Anyway, one day this teacher, with his supervisor present, was making a presentation to the class when, suddenly, two dozen pop-ups of tubgirl.com came onto the screen. Much laughter (of the students) ensued. To this day, our is "network manager" baffled by this. It was all done through the wonders of psexec, which will remotely execute a program on a target machine. If necessary, it will also copy a program to the remote machine and then execute it; however, I have not been able to get this feature working correctly. The other utility, psshutdown, will remotely log off, restart, or shutdown a target machine; you can also provide a list of machines in a separate file. You can download all of the Pstools and read the guide on the syntax of their use at `http://www.microsoft.com/technet/sysinternals/utilities/pstools.mspx`. Once again, you can make some nasty automated batch files with this. Here's a good example with what I like to call the "SuperShutdown". Make a batch file with the following code:

```
psshutdown \\* -u username -p password -k -f -n 10 -t 9:00 -v 0
```

This will effectively shutdown every machine in the same Windows domain as you at 9:00 a.m. The time is in specified 24-hour format. You'll also need to use an administrator's username and password, which you conveniently got with pwdump2 and john if you read my last article, for this to work. The other parameters are `-k` to shut down the machine, `-f` to force any applications running on the machine to close, `-n 10` to specify the timeout connecting to remote machines because psshutdown won't work on Windows 98, and `-v 0` to disable the dialog that appears when the machine is being shutdown. Make sure you don't forget the `-v 0`; otherwise, a dialog will display on their machine that you from your machine are running the shutdown!

As always, use your head when playing around with this stuff. You can play some great pranks with psshutdown and psexec, but pay careful attention to the various switches and parameters they have; forgetting or misusing one is an easy way to get yourself caught. Speaking of getting caught, if you are captured by enemy sysadmins, any knowledge of your existence will be disavowed.

PAYPAL HURTS



by Estragon

This article is about how PayPal transaction reversals can cost recipients a lot of dough. I'm writing from the perspective of a hacker who sees how the shortcomings of the PayPal system could be used to take money out of the pocket of someone else.

The techniques described in this article could be used against anyone with a PayPal account, in amounts from a few pennies to thousands of dollars. With a mass protest against, say, a disfavored political candidate, company, or individual, many people working together could rapidly cause trouble—including plenty of money lost—for their target.

My biggest concern is the "Donate Now!" button linking to PayPal that we see on the websites of so many charities and open source software development projects. I was inspired to write this article when I received a chargeback, and later a transaction reversal, from PayPal. I run a charity that operates an open source project, and receive donations via PayPal. Getting donations via PayPal is quite nice, and it's a major way we sustain our project.

The basic situation is that on PayPal it costs a recipient extra money when a transaction is disputed by the sender. While this isn't that different from the way banks and credit card companies operate, many individuals and small charities use PayPal because they can't afford the infrastructure, don't have the volume, or haven't got the right type of corporate structure to accept credit cards directly. In other words, this technique can be more hurtful with PayPal against small charities or similar organizations than against bricks-and-mortar stores.

For money that was paid and received by PayPal (from one PayPal user to another), PayPal handles disputes internally. So, if funds were sent to you from someone else's PayPal account, and the transaction is disputed, PayPal has a process to evaluate the claim. You can find their resolution process online, with lots of details. It is very much geared towards the selling of goods.

Here's the rundown of an actual disputed transaction I received recently. Someone made a $2 donation to my organization, then filed a dispute.

For a $2.00 purchase or donation sent via PayPal with a PayPal account, $0.38 was charged as a fee to accept the payment, then $0.38 was charged to reverse the transaction.

PayPal walked away with 38 cents (19% of the original transaction), and my PayPal account was 38 cents lighter as a result of the transaction. The $1.72 netted originally from the $2.00 donation was removed, but then a further 38 cents were removed.

PayPal also accepts payments via credit card. If a credit card transaction is disputed, the credit card company interacts with PayPal. PayPal interacts with the PayPal account holder.

If the transaction is reversed (in this case, it's called a chargeback), a chargeback settlement fee may be charged if the credit card company charges PayPal. That is, PayPal passes the fee on to the account holder. In what became an actual chargeback, I received a donation of $100 which was disputed about 10 weeks later and subsequently reversed.

For a $100 purchase or donation sent via PayPal with a credit card, $3.20 is charged as a fee to accept the payment, then $3.20 was charged to reverse the payment, then $10 was charged as a chargeback fee

PayPal walked away with $13.20 (13.2% of the original transaction), and this time my PayPal account was $13.20 lighter as a result of the chargeback. The $100 donation via credit card cost lots more than the $2 donation via PayPal account if there is a dispute and chargeback.

PayPal charges fees as a percentage of the transaction. Normally, this is 30 cents per transaction, plus 2.9% of the transaction. There are variations in different countries, for different currencies, and for different types of transactions.

Doing the math, if ten people worked together to each make a $100 donation, then made a claim against me, I would be out $132, rather than receiving $968. Below, I'll give some ideas about how such mass action could happen with relative impunity.

To sum up, the chargeback (involving someone who made a donation to my organization via PayPal) had these costs. First, the amount of the original donation was removed from my account. Second, PayPal collected their usual fee (described below) on the transaction amount—even though they had already removed it off the top from the donation amount. Third, there was a chargeback fee of $10 from the credit card company.

In my research, I found that PayPal lists different chargeback fees for different countries (they're all about $10-20 US). Some banks list their credit card chargeback fees, which are comparable and sometimes even higher.

How can you work around losing money through disputed PayPal payments? If you're actually selling items via PayPal, follow the terms of their Seller Protection Policy. Read the fine print: protection stops for many purchases at $250.

Protection does not extend to anything other than goods. PayPal's seller protection plan states that "Only physical goods are covered by the Seller Protection Policy. Intangible goods, such as services or items delivered electronically (e.g., software, MP3s, eBooks), are not covered." In other words, there is no seller protection plan for accepting donations, taking payment for work performed, or other non-tangibles.

There don't seem to be dollar limits for seller protection, and I have made and received payments of up to $10,000. But for buyer protection, transactions are only covered up to $2000 under certain circumstances, $250 otherwise.

During the time of a dispute (which can take

weeks or months, but is more typically just a few days), the payment amount is frozen.

PayPal has a policy that they do not reverse PayPal transactions unless they are taking money from the seller. In other words, it's not like US banks' FDIC insurance. Imagine that someone scams you for $1000 from your PayPal account, then withdraws the money from their PayPal account, leaving it empty. PayPal will not give you your $1000 back unless the other account has that money. This opens up a whole lot of possibilities, but it's basically all just fraud: take the money and run. There are many stories about this happening on eBay (which owns PayPal). From reading PayPal's policies, it sounds like it doesn't matter whether their "buyer protection plan" applies or not.

Compare this to credit card protection, where you will get your money back regardless of whether the credit card company got their money back, or whether any goods involved were returned. Your mileage may vary, and things might be different outside of the US. My few experiences with credit card fraud were that the credit card companies just didn't care: they would hold a transaction during "investigation" and do essentially nothing. At the end, if the merchant fights, the customer loses. But if the customer wins, the credit card company will return the money.

On the two occasions where my credit card was stolen (once physically, once electronically), I provided proof (a police report #) and the charges were reversed. The legitimate stores that were stolen from (with my credit card) was not given their money for the transactions, and did not get their goods back. One of them was assessed a chargeback fee by the credit card company, indicating that the PayPal technique described here can be effective with credit cards, too.

By the way, if this hasn't convinced you to never use your debit card for these types of purchases, you need to read your debit card agreement. Most banks offer very little protection for debit card transactions, even if the debit card holds a major credit card seal.

Let's work through some exploits. First, imagine a hypothetical candidate running for national office. The candidate accepts PayPal as a method of donation on his or her Web site. If ten people each make donations of $1000 to the candidate, using their credit card, the candidate will have $10000 minus PayPal fees of $293.

If those ten people then call their ten different credit card companies, saying the charge was unauthorized ("my teenager borrowed my card," "I think the Starbucks store I go to every day might have copied my card number," etc.), the candidate will lose the $10000, plus another $293, plus another $100. Ten people together cost the candidate about $393 from his or her own account.

Would the credit card companies catch on? Probably not, for two reasons: the excuses given are not big enough to warrant serious investigation, and there is not a lot of sharing and reporting of credit card fraud. Will PayPal catch on that the ten people are working together? Maybe, but what if they all had a common excuse ("we all go to that Starbucks")?

Second, let's look at a larger scale with smaller donations. What if a fraudster has hundreds or thousands of stolen credit card numbers, and a vendetta against a particular open source software project's charity? Assuming the criminal had plenty of time on his or her hands (since it's intentionally hard to automate payments and account creation on PayPal), she could run a few transactions of less than $10 per day to the targeted charity. Then, let the legitimate credit card holder dispute the transaction.

At $10 per chargeback plus fees, any donation of under about $11 is a net loss for the targeted charity of the chargeback fee, in addition to the cost of the reversed transaction.

Finally, let's think of an even larger-scale scam. How about an urban legend sent via tons of spam? Message one: "This charity is doing wonderful work, but is about to have its charitable organization status reversed by the IRS. In order to meet the IRS requirements [insert valid hyperlink here], they need to receive several hundred small donations ($2 to $10). By donating with your PayPal account or credit card, the charity will be able to provide clear proof to the IRS that the charity is legitimate."

Link to the real organization and its real PayPal link. Wait for people to donate. Assume a very small (less than .1%) response on the spam but a large campaign of millions of spams. There are clearly a lot of idiots who respond to spam, and you only need a small proportion.

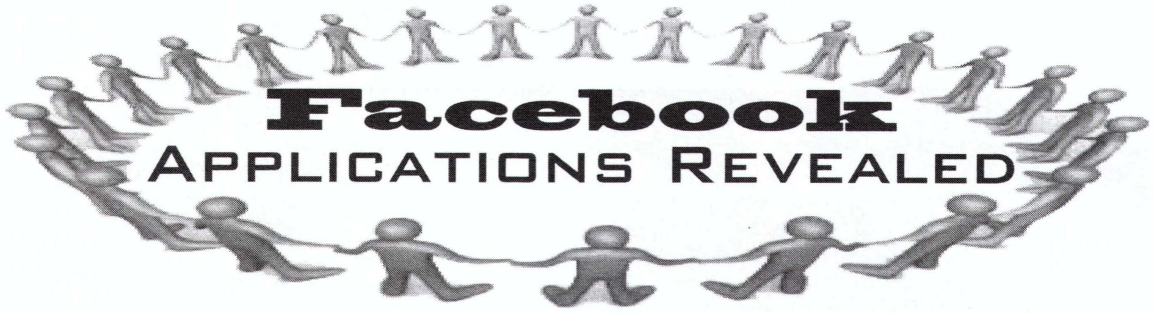
Then, a week or two later send spam message #2, "You might have heard recently about a charity that made a plea to maintain its status with the IRS. If you donated any money be informed that you are a victim of fraud. The charity's IRS status is not up for renewal, and there is no effort to remove its 501(c)(3) status under IRS regulations [insert another valid hyperlink here]. If you donated with PayPal, protest your donation and reverse it, follow this link [link to PayPal dispute center]. If you donated with your credit card, be sure to file a dispute claim with your bank."

Would your spam campaign bring in more money to the target than was reversed later? Again, let's do some math. Assume 200 donations are made with an average of $5 each, and 50% of donations are made via PayPal accounts, with the others are made using PayPal with a credit card. The net gain is 200 x $5, minus 45 cents per transation for PayPal's fees: $911.

If 100 out of 200 donors file a successful claim with PayPal or their credit card company, and half used their credit card, $500 would be removed from the charity via PayPal. Chargeback fees would net a further $500 ($10 each for 50 credit cards). Further PayPal fees of $48.50 would be assessed as the $500 were removed. Total removed is 500+500+48.50=1048.50. The charity would get to keep the proceeds from the 100 donors who didn't protest, about $455.50 (half of $911). Net loss to the charity is 455.50 - 548.50 or $93.10—plus lots of aggravation.

PayPal does have a lot of protections in place, but far fewer when no goods are being sold, and far fewer at larger dollar amounts. Just a few reversed transactions can make a charity or other recipient have bad day. In this article, I have laid out some of the basics, and also worked through some hypothetical scenarios where a larger number of reversed transactions can be truly damaging.

Lots of people have worked on anonymous payment systems, non-repudiation of payments, and escrow systems for delivering goods. For examples, read some articles on e-gold. PayPal does not implement the hard parts of such a system, which require a trusted intermediary (not one who profits from every type of transaction, including illegitimate ones, as PayPal does), and strong cryptographic methods of ensuring identity while maintaining anonymity. PayPal is ubiquitous, but has flaws. Let the buyer, and the seller, beware.



by stderr
stderr.dev@gmail.com

0x00: Introduction

Surely most of you are familiar with Facebook, one of the most popular social networking sites on the Internet. Many faithful users once praised its simplicity and its elegance. Then, one fatal day in late May, Facebook unveiled its development platform, unleashing a flood of third-party application add-ons to the masses registered on Facebook. Thousands of eager users mindlessly added these feature enhancements. Many of Facebook's most faithful users began to get agitated with all the traffic coming from their friends, who were starting virtual food fights, and in some cases even began virtually biting friends (creepy). Along with the shear annoyance of these applications, a new question of security was introduced.

Now that you have all of these neat gadgets at your disposal, what else are you allowing onto your page? Facebook's application help page states that "...applications built by third parties do not affect the privacy of your information in any way. Your account information is still secure and we ensure that no third parties store or collect any of your information."

As Facebook stated, your stored information is safe, but how is the authentication on the applications themselves? This is left completely up to the plugin developers. As we will see shortly, many developers did not take security very seriously as they developed and released these applications.

Due to the overwhelming number of applications, we are only going to take a look at three sample Facebook applications. These applications should give you an idea about some of the privacy and security issues that come with adding Facebook applications.

0x01: Firebug

Before we begin, I highly suggest that you download the Firefox plugin called Firebug. It is an amazing tool that allows you to develop and debug websites. More importantly to us, it allows you to alter the client-side code before submitting a form. In order to jump to a place in the code, right click on the desired section of the page and click "Inspect Element." There are several ways of altering the pages given below, but this seems to be more efficient than manually editing the GET variables in the given URLs.

0x02: Moods

The first application we will look at is simply called "Moods". Moods is a very simple application that allows you to set your current state of mind and display it to your friends. A neat feature includes the ability to store the history of your past mood settings and changes.

This application seems simple enough. Where could there possibly be a security lapse? I am glad you asked.

First of all, when you view someone's mood history, the application does not ensure that you are a friend of the person whose history you are viewing. Okay, big deal: someone can see the history of my past moods. I couldn't care less! Well, anyone could easily automate the task of grabbing everyone's current mood. Subsequently, this could be used in conjunction with other data for future phishing or social engineering attacks. For instance, people that are currently depressed or confused may tend to be more prone to falling for something stupid.

To see someone's moods history, simply substitute the target's Facebook id where the Xs are:

```
http://apps.facebook.com/emoting/
➥?page=history&uid=xxxxxxxxx
```

Thank you for hanging with me this far. Hopefully this example motivated the hamster to start running in your head. If you are following my thought pattern, the next logical step would be to try to set your mood and see what happens. When you click the icon to set your mood, a URL like the following is used to update your status:

```
http://neo.hotornot.com/facebook/
➥emoting/set_mood?emo_id=xx&fb_sig_in_
➥iframe=1&fb_sig_time=1183868333.4734&fb_
➥sig_user=xxxxxxxxx&fb_sig_profile_
➥update_time=1183845237&fb_sig_session_k
➥ey=ljaoduf982309audsoifuiaj34iajidjdd&
➥fb_sig_expires=0&fb_sig_api_key=ao3o2au90
➥ua0983209809809832098l3&fb_
➥sig_added=1&fb_sig=3ljaljds
➥ioajljl3223209a0932a4abe
```

Yes, you guessed it. Moods does not authenticate to ensure that you are setting your current mood. Simply change the `fb_sig_user` variable to another person's ID, and you can update how they are feeling. Do not tell me how I feel!

0x03: Free Gifts

Facebook came out with a feature that allows you to give virtual gifts to your friends. Maybe you want to send a picture of a rose, a picture of a hamburger, or a picture of handcuffs to your friend. That is all fine and dandy, but then Facebook decided to charge you $1 per gift. Most of us are too cheap to actually pay $1 to send a stupid picture to someone on the Internet. Enter the Free Gifts application.

Free Gifts is just as the name would suggest. It is an add-on that allows you to send and receive free gifts to and from your friends. The flaw in this application is eerily similar to the one found in Moods. You can view the gifts received by anyone (friend or not), simply by altering the id number sent to the Facebook application: `http://apps.facebook.com freegifts/?to=xxxxxxx` Again, simply change the id, and you can view that person's received gifts. You may have guessed it by now, but you can also send a free gift to any person that uses the Free Gifts application, friend or not.

You probably noticed while looking at some random person's received gifts, that there is a "Send a Gift" button on the top left portion of the page. Sending this person a gift is not quite as easy as simply clicking the button, but it might as well be. After you have clicked to send a gift, select the gift to send. Now, you have to choose a recipient. Select from "Friends With Free Gifts". You might notice that if a person's not a friend, then you can't send them a gift. Now is when Firebug starts to shine. Right click on the drop down menu of friends and inspect the element. You will see a list entry like the following.

```
<option
value="xxxxxxxxx">MyFriend</option>
```

Simply alter the values to reflect the person that you want to send the gift to. You can send the gift anonymously, or you can just be a creepy stalker and send the gift from your own profile. So far we have been able to view or change anyone's mood, and we have been able to send gifts to anyone with the Free Gifts application. What comes next?

0x04: Super Wall

When you setup your Facebook account, they give you a virtual "wall" where friends can post public comments to your profile. This is kind of cool, but there are some limitations. You cannot post an image or a video to a friend's wall. Well, the inventors of Super Wall have come to the rescue. This application allows simple text messages, picture messages, and even links to web videos served up by Google or Youtube.

My original testing with Super Wall included trying to link to an off-site image, in an attempt to track profile views. Facebook counters this by caching every image used in third party applications. Therefore, all requests to images are effectively handled locally by Facebook's web servers. This helps reduce the server load on any third party websites.

Since my first attempt was shot down, I decided to look into other aspects of Super Wall. For my second test, I posted a simple text message to my own Super Wall. Awesome, everything is working. Finally, I took a look at what was going on behind the scenes.

Firebug came to the rescue again as I inspected the Post button for the Super Wall application. Interesting:

```
<input type="hidden" value="xxxxxxxxx"
➥name="fb_sig_profile"/>
<input type="hidden"
➥value="1183832316.0082"
➥name="fb_sig_time"/>
<input type="hidden" value="xxxxxxxxx"
➥name="fb_sig_user"/>
<input type="hidden" value="1183835287"
➥name="fb_sig_profile_update_time"/>
<input type="hidden" value="134
➥0983509832098109284098320958203
➥" name="fb_sig_session_key"/>
<input type="hidden" value="0"
➥name="fb_sig_expires"/>
<input type="hidden" value="223413441509832
➥10981039859083235"
➥name="fb_sig_api_key"/>
<input type="hidden" value="1"
➥name="fb_sig_added"/>
<input type="hidden" value="23919218214
➥912931049381098314893" name="fb_sig"/>
<input type="hidden" value="XXXXXXXXX"
➥name="owner_id"/>
```

The `fb_sig_user` field is the Facebook user id of the person posting the comment, and `owner_id` is the Facebook user id of the Super Wall's owner. When writing to your own Super Wall, both of these fields will be equal to your Facebook user id.

Unlike the previous applications, Super Wall ensures that you are on the person's friend list before you can post to his or her Super Wall. However, if you change the value of `fb_sig_user` to a friend's id, the result will be a wall post from your friend. You have now spoofed a comment from one of your friends onto your own wall. Wow, this could get ugly.

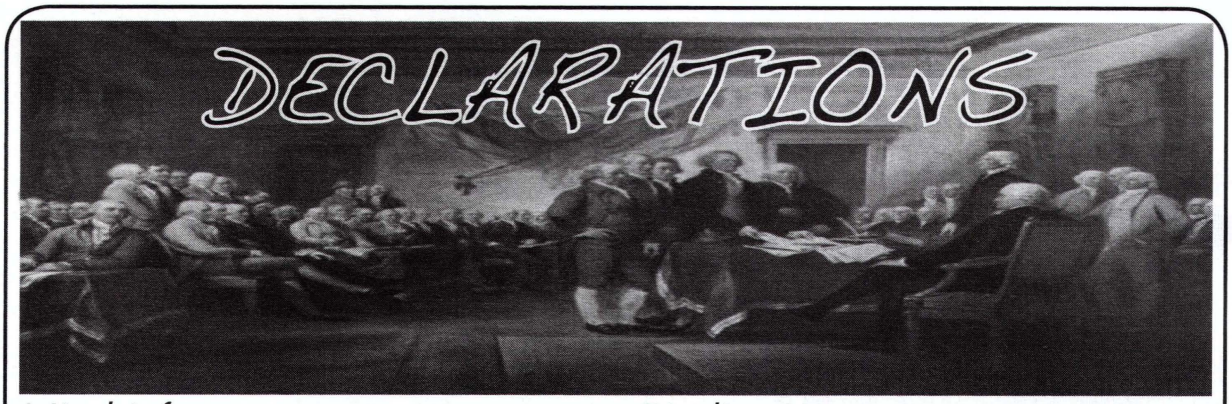
After further tweaking, I was also able to post on a friend's Super Wall as someone else, simply by altering both the `owner_id` and `fb_sig_profile` fields accordingly. The person you are posting as does have to be a friend of the wall's owner in order for this to work.

Phishers could easily abuse Super Wall by spoofing messages to people by assuming a friend's identity. The phisher could then post malicious links, and the victim would likely not even think twice about going to the given address. Spammers could also automate posting messages from friends to people's walls. One way developers could help defend against this attack is by adding a picture box confirmation tool that would be presented before posting the messages to the walls.

0x05: Conclusions

We just finished up with a quick look into some of the security concerns with Facebook's new third-party applications. There are hundreds of available add-ons, and looking at the security on all of them is something I will leave up to the readers. These security lapses could easily lead to spam or phishing attacks on you and your friends. Thanks to the new applications, it is now possible to pose as someone else, without ever cracking a password. Please think twice before adding another application to your Facebook profile. Embrace simplicity.

Shout-outs: Everyone at BinRev, venom, ny0n, Dan, Todd, Michelle, Anna, and all my college friends.



Mischief

Dear *2600:*

Here is something extra to add to my article in 24:3 ("How to Cheat Goog411"). One really cool and easy thing to do is to register a business in some faraway place with a name like "Tennis" or "Golf" or something simple like that. Then what you do is call up Goog411 and tell them the city/state of where you added that business. But when it asks for a business name or category, just yell anything into the phone. Make sure it doesn't register what you said. It should say "I'm sorry, try again" or something similar. So yell something incoherent into it again. This time it will say "If you'd like to type in the business name or category using the keypad, please press 1." So you press 1. Then you use your keypad to type out your business name - "Tennis," "Golf," or whatever, and, if Google picks it up, it looks for a business named that. Since you put your business in an obscure city/state with a name so generic as "Golf," it will probably pick your business. This is one of the best ways that I've found to make sure that Google will pick your business. Cause it always thinks you're typing a business name. Very surefire way of getting Google on your side.

Good luck, and happy Google hacking.

PhreakerD7@gmail.com

Dear *2600:*

I was stuck in Schiphol airport (Amsterdam) a couple of weeks ago and had a chance to screw around with a web terminal near my gate. I didn't really need to get on the web enough to justify the two euros for 15 minutes or whatever it was, so I figured I'd try to score some for free. Here's what I came up with. So simple you could follow even after a trip to the smart shop:

1. Press Windows-u (opens accessibility options).
2. Click "Help" button.
3. Right click the title bar.
4. Select "Jump to URL".
5. Enter a valid URL (must include protocol).
6. Enjoy your free Internet.
7. Even better, browse a website that opens links in a new browser. Click one of those links and you have your very own IE window.
8. Have fun. I didn't have much time, but I did get a chance to play around with the Internet settings (new home page!). I'm sure you can get away with much more.

mthed

Binding Woes

Dear *2600:*

I would like to voice my complaint about the new binding you are using. I received the last issue of your magazine in the mail and read it from front to ten pages before the last. Around page 55 I discovered that the pages where being torn from the binding. I don't mean to say that they were coming unglued, they were actually ripping a millimeter or two away from the glue.

Please find another binding solution or stop putting the words so close to the middle.

XeNoS

Words cannot express how upset we've been at the problems with the past issue. Apparently the inside paper was too thin while the cover had the proper thickness. We've made a bunch of changes and expect to get this one right. Let's hope the page you're reading these words on does our magazine justice.

Dear *2600:*

I have always enjoyed reading your magazine. I have even resubscribed recently because of the recent closure of my favorite local magazine store. The new binding absolutely sucks. I can't even open the damn thing without it becoming impossible to read the words near the binding. The pages are even starting to fall out on the latest issue. Raise the price and go back to the old binding.

Andy

If the problems don't go away we will have to look at other possibilities. At this point it appears these annoyances were caused by using the wrong type of paper and miscommunication as to what the proper margins should be. If the letters are too close to the margin or if the paper is all screwed up again as you're reading this, there's a good chance someone is being harshly interrogated on the matter at this very moment. We apologize to everyone for the Autumn issue which we consider to be below our standards. We've made a lot of changes and we hope to see results with this new issue. Thanks for sticking with us.

Discoveries

Dear *2600:*

So I think I've solved the puzzle from the Summer issue. "The Thinker" is thinking about how much he hates the DMCA. I am sitting here thinking about how much I just learned about the data matrix format!

I started by trying to reverse engineer the entire thing by hand. I was at "work" so I used the tools at

hand: a text editor and PHP. I created four arrays of data with a 1 in each piece of the grid that was black and a 0 for each piece that was white. (What can I say - I was at work and bored. Besides, doing the data entry reminded me of stories I'd heard of people hand coding Commodore games by typing in the byte code out of magazines!) I then started trying to see some patterns in the numbers based on the decimal value of the binary value of each row. I quickly discovered there were some numbers vaguely close but nothing that matched. I then tried making a composite of the arrays. This yielded four or five pieces of "the matrix" that were empty but nothing meaningful. I printed it out and took it home. I realized that the left, bottom, top, and right bars seemed to be uniform for each sector. I noticed this while entering it manually as well. I figured these must be "registration" bars or whatnot for some type of scanner. I also flirted with the idea that maybe the decimal values could represent words in a base 18 notation or something similar. I slept on it.

The next morning at work I went to wash my hands in the bathroom and was checking if the soap was vegan or not (seriously) and noticed a pattern that looked very familiar to what I had been staring at all night. I knew I had seen something similar before. I spent the next couple of hours researching alternative barcode methods and finally stumbled upon the data matrix. I spent a while reading about decoding algorithms which compensated for poor image quality, etc. This wasn't an issue for me as I manually inputted them and then had a function which generated the image, not with GD, but with a table with divs set to 8x8 with a background color of black. I made a screen shot and cropped it down, then I found an online utility which can encode and decode data matrix images. No joy. It just returned a blank string! I though for a moment maybe the data matrix did represent nothing and it was supposed to be some sort of Zen koan like "form is void, void is form" type deal - haha. I double-checked that I hadn't entered any info wrong and as far as I could tell I hadn't. An hour later I read something about needing a "quiet zone" around the image for any of the algorithms to work. I added a white border around the image and tried it again. Bam! I finally got an output that meant something!

The output translated to 09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63-56-88-c0.

That joyous number! That number which brought Digg to its knees a few weeks earlier. How could it not be burned into my mind forever? So yeah, I hope that suffices as an explanation as to how I figured it out, etc. And I guess my final answer is that the thinker is thinking "Fuck the DMCA." Never give up, never give in, never let the enemy win.

shaunxcore

It is indeed heartening to see how much time and effort people spend in solving these things. We're sorry that you didn't actually win this time but we trust you had fun on the journey.

Dear *2600:*

It may amuse you to know that "2600" is the postcode (zip code for you Americans) of Capital Hill, where the Australian Parliament is situated.

Chris

So technically every time they convene it's a 2600 meeting.

Dear *2600:*

Here's an interesting tidbit for your readers. Boston's transit fares are collected using a system of magstripe paper tickets or RFID plastic cards. I was having trouble with a paper ticket and I'm pretty sure I got double-charged for a trip. So I talked to one of the transit workers at a station to ask what he could do.

He brought me to one of the ticket machines and did something to get to a screen that asked for his PIN. Then, as I watched, he started entering his PIN right in front of me. I started to look away out of courtesy but, to my shock, he actually said the numbers out loud as he entered them!

Entering his PIN got him into an administrative mode that, among other things, allowed him to get detailed information on when fares were deducted from my card. Sure enough, we could see the double-charge... not that he was actually able to do anything about it. How annoying.

For the curious out there (and who isn't?), the PIN was 13210. I'm not sure what he had to do to get to the PIN entry screen, but I'm afraid it might have involved tapping his special administrative RFID card. I wasn't paying attention, though, so it might only be a matter of tapping a special button. Certainly it wouldn't be hard to pretend to be in a situation like mine in order to watch a transit employee more closely while they access the menu. It's interesting that their security is so lax. Of course, that's not an excuse to use this information to get free fares.

Lex

People who speak their PINs out loud almost have to be admired for completely moving in the opposite direction as the rest of us, who are forever trying to become more secure and protecting our private information (and that of others). We wonder how many other PIN talkers are out there.

Dear *2600:*

This is a very simple hack, but only works if you already have a resident login to this system. ISTA North America is a third-party utility billing company that bills residents for utilities on behalf of apartment buildings. Simply go to www.istabills.com, login, or sign up for a login using the account number on your monthly bill. Once logged in, click on "History Prior to (whatever date)." This will take you to the old access page, which can also be accessed directly at http://accountsjax.viterrausa.com. You can also login here with your account number and PIN, or sign up for access with your account number and other information. Once logged in, click on "Display account history." You can then proceed to display the account history for any resident account simply by changing the "LOC=" and "ROUTE=" values in the URL. The site does not use cookies to keep track of users, nor does it use SSL. The ROUTE value is the property ID, and the LOC value is the resident ID. You can also click "Change password" or the other options from the main account page and reload the pages using different ROUTE and LOC values to change other users' passwords and so forth. These pages were obviously last used in 2006, but since they're still up, they pose a security and privacy risk that was brought to this company's attention over a year ago and which they refused to act upon.

a a

In addition to this flagrant violation of privacy,

new users are told that their "User Name is the Service Code printed on your utility bill" while their password is simply their five digit zip code! After getting this easily obtainable information from some unsuspecting person, there's no end to the havoc that could be caused.

Dear *2600:*

I'm currently at a halfway house in Oklahoma. I figured out a trick with the phones here and now everyone calls long distance for free. But what I'd like to know is what kind of system are these phones based on that would allow us all to make free calls? Here's what we do: we pick up the handset and dial 18, count to three slowly or wait for a tiny click from inside the phone (I have to count because I'm hard of hearing), then press 00 and quickly press one or two numbers eight times. (I like pressing 7 and 8 back and forth... makes a cute jingle.) An operator will say "thank you" and if you did it right it will say "thank you" again and give you a dial tone. You can then call wherever except for international for some reason. I can call Canada though. Sometimes it makes a loud whistling feedback noise and sometimes it gives you a dial tone but the keys don't work. Could you clarify what's occurring for this to happen?

I love your mag and still get it even though I'm incarcerated.

Noah

It's hard to say exactly what's happening but there's surely some sort of a drop down to a dial tone at some point which might be the tiny click you hear. Or it could be the dial tone you get after the "thank you" which is bypassing the normal restriction. Then again, dialing 18 could be connecting you to a distant line somewhere. The important thing is that you're continuing to use your mind and figure things out while incarcerated which is always a good thing to do. These days getting around dialing restrictions is less about the cost and more about just bypassing whatever controls are being placed on you. In a world where you can have unlimited long distance for next to nothing, these kinds of controls shouldn't even be around much longer. At least not for reasons of cost.

Theories

Dear *2600:*

I am writing about possibly getting an article posted. I believe that this would make a worthy article for its controversial nature and its unending curiosity. I have always found the idea of time travel plausible. It has always been on the back burner in my mind trying to figure out how and why. So I am asking that you give a moment of your time to read a story/theory about time travel. I think it would be worthy of readers' time as well. After the publishing of H.G. Wells' book The Time Machine, science has embraced a new study. Throughout time they have become more and more aware that this might not be so farfetched. Scientists are believing that they are getting closer to unlocking the mystery and making it possible to indeed time travel. Many theories have been presented over the years and I would like to share mine with you now. First off, I would like to eliminate the idea of using a De Lorean car (as in Back to the Future) to time travel. I would also like to eliminate the idea of a time machine that can travel both forwards and backwards in time. I state that because time is a constant. It is always moving forward. Chronological events in history easily verify this. Now that I have cleared up those little misconceptions, I would like to move on to the bigger picture. To make time travel possible we are going to need a vessel that can carry us. This would look no different than your average space shuttle with minor alterations. For example the engines may be different and the gas chambers larger to hold the amount of fuel that is going to be needed to make this a reality. Now with our shuttle built, we need to discuss how it is going to be used. Assuming that the shuttle was built to execute our plan, we are going to need to travel away from the Earth at a speed faster than the Earth is traveling. Time on Earth is only relative to the speed the Earth is traveling. We manage our time due to the spinning. By traveling this speed (assuming that there is enough fuel to propel us that fast and for the amount of time), we are able to create a difference in our time and Earth's time. Time now having a different factor for us, we can imagine that the Earth is aging more than we are at a faster rate. It is as if we are slowing down time due to our speed. Without precise calculations we are not able to determine the amount of time we would be exceeding during our travel in space. Upon returning to the Earth, assuming that the theory is correct about time being different for moving objects and the speed they are traveling, we can infer that the time we have aged would be less than what the Earth has aged. It may not be the fountain of youth, but it is a step up. Remember that this is only a theory. There are kinks and ideas that are subject to change. Thank you for your time.

Jesse

It's good to hear that scientists are exploring the possibility of time travel without the use of a De Lorean as they are rather expensive and difficult to get a hold of. We also are indebted to you for confirming that time travel is indeed a one way street. This easily explains why we have not met any time travelers since they would have to come from the past where it hasn't been invented yet. We look forward to future reports from the laboratory.

Dear *2600:*

I just activated "my favs" on my cell phone and the difference I noticed was when you add a number to "my favs" it adds a + in front of the phone number. So if I am not mistaken if you hold the 0 for a couple of seconds, the + comes on the screen. Then you dial the number you want and send and this should make a call without any extra minutes as it will be a "my favs" call. So in other words + is no minutes charge or + is a plus.

Ken

The plus sign has nothing at all to do with billing the call. On GSM phones, the plus sign can denote the beginning of the phone number. It can be gotten in various ways, by hitting the asterisk button twice, holding the zero, and through other methods. It's usually followed by a country code and then the rest of the number. In the States and Canada we have it easy since the country code is 1 and our dialing "1+" in front of most numbers as part of our long distance format achieves the same effect as dialing from overseas on a mobile phone. The plus sign also won't interfere with normal domestic dialing so it's transparent.

Dear *2600:*

I'm not a hacker per se but need to bring forth a little information and start a serious discussion for our future. Over the decades, bionic implants have become more popular. Electronics have found their way into our eyes, brains, limbs, and our hearts. In such a pioneering field of research, security and safety from a hacker's point of view will take a back seat. Let's take a look at how current technology is exploitable and ultimately life threatening.

Pacemakers have been implanted since the late 50s. They have an onboard computer called the generator. When the generator senses an abnormality in the heart rhythm it triggers a lead to contract the muscle. Back then these "rate-responsive" devices were set to trigger at preset numbers. An example is if the heart rate drops below 70 pmb the device starts to pace. The generator reads body movement and breath to determine what the pace should be. The thinking is, the more you move and breath, the more your heart pumps.

New pacemakers are a little more flexible. They have a magnetic switch called a reed. A small magnet producing more than 90 gauss can close this switch. This puts the device into programming mode. Coincidentally, once closed the device sets to a default pace. To my knowledge a person's heart rate drops pretty low during sleep. It would be a shame if a magnet got close to the left collar bone. The last thing you need is a pacemaker doing 45 bpm while your own heart is trying to do 38. Arrhythmia sounds painful even to a healthy heart. You'll want to stay away from arc welding, cell phones, large motors, MRIs, etc., etc.

Another avenue for attack is the actual programming of the device. A simple web search can lead you to the handheld programming equipment. You can also get a monitor transmitter from eBay. These transmitter devices are placed near or connected to the pacemaker's generator. They convert and transmit information via telephone to a physician that reads device/patient statistics. My knowledge stops there. My point is this. The pacemaker is a simple device that one can use to cause great damage. I'm not talking about hacking a door here; this is a life. As implants become more advanced and common in our health and pleasure, I hope patient safety outside the medical procedure is considered.

kiX

Responses

Dear *2600:*

This letter is in response to the aspiring corrections department officer regarding Jack McClellan, the self-proclaimed but not legally convicted sex offender.

McClellan has previously stated in interviews he created the website www.stegl.org (Seattle-Tacoma-Everett Girl Love) as a way to inform parents about their lack of attention to the safety of their children while out in public. Depending on who you believe, McClellan stated he removed the website because of the flack he was getting but others say it was the service provider which removed the site.

Shortly afterwards he moved to California where he started a similar website called Los Angeles Girl Love. California stepped up to the plate and issued a temporary restraining order requiring McClellan stay 30 feet away from any child.

This is where things could get tricky.

In most courts, for a restraining order to stick, the petitioner (person obtaining order, in this case attorneys with daughters) needs to convince the court the respondent (person the order is against) poses an immediate threat to the petitioner. How can McClellan be considered a threat when he takes his photos while out in public using equipment you can buy at any store? Is this where we start arresting people and convicting them on the mere fact they might commit a crime?

Or is it a situation in which McClellan has committed a crime, despite his cries of innocence, and just hasn't been caught?

Talk to any law enforcement officer, corrections officer, probation officer, or attorney and find out how many attempts it may take for a crime to actually stick to a criminal's record. Your chosen career path is a thankless but noble path. Stick with it because in the end the criminals do get their justice. And no vigilantes are required. Good luck.

Squeeling Sheep

There are real dangers in taking shortcuts to justice and that's what the above case demonstrates, whether intentionally or not. While this guy may now be on everybody's radar, any sort of a prosecution without a clear-cut violation of a law would do far more harm than good ultimately. This sort of thing is mirrored in all sorts of other cases where people who are pretending to be a certain age are prosecuted for potential crimes against someone else who's also pretending to be a certain age but is actually a law enforcement agent. And while there may be a 95 percent chance that a crime would have been committed had the second person actually been a minor, the inconvenient fact here is that there was no real victim - actual or potential. Many are willing to overlook this little problem in the interests of safety and peace of mind but it's a step in a disturbing direction. One day we could actually see prosecutions for such things in the "Second Life" world, among other places, where the people aren't real but crimes against them would be.

Dear *2600:*

I have been an avid reader of your magazine for quite some time. Most interesting to me is the opinions section. Reading the suggestions, comments, and questions always brings a smile. In this past issue the very last opinion posted is a question asking "What OS do you prefer: Windows, Linux, or Mac?" The *2600* response is "We don't discuss religion here." I must tell you that this comment had me laughing hysterically. I found that likeness to be so absurd and yet the more I think about it the more it becomes appropriate. Why is it that we must define ourselves by what OS we use? Let us not divide ourselves into small fractions of a community but exist equally with all who are electronic enthusiasts. Hackers are first and foremost for the freedom of ideas and information everywhere. Hats off to your entire team for the excellent work you do in taking part in the freedoms we can all enjoy.

3v.mike

That sentiment sounds suspiciously Debian.

Dear *2600:*

To daColombian:

After all is said and done, you're still fetching images

from www.2600.com for display on your browser and that domain would still be showing up in any log files that your network admin keeps. You're no better off than if you'd just bookmarked it unless your admin also enjoys poking around in your browser settings. If 2600's main web page really is too slow to load over dialup, I suggest you subscribe to the RSS feed at http://www.2600.com/rss.xml and watch it for publication notices (and other interesting news!). At less than 8kb as of today, even a slow modem should be able to download it in a couple of seconds. *To "M" in the opinions section:*

I live in a small town. I am a sysadmin and my wife is a doctor, so we're both on call pretty much 24/7. We like doing the same things you and your friends do, including going to movies. Our cell phones are always on vibrate in theaters and other quiet public places and neither my wife nor I have ever once answered them without first stepping out into a hallway or lobby. If cell phone jammers become common, we would never be able to enjoy an evening out again; being reachable in case of a work emergency is more important than the new Resident Evil movie.

I know that some impolite jerks don't care if they ruin it for the rest of us, but don't take it out on the majority of us that act responsibly. Remember, you don't hear all the people in a theater who have their phone ringers off or on vibrate. You just hear the idiots.

i<3puppies

In some places, theaters and restaurants themselves are the ones that operate cell phone jammers. In addition, there are lots of places that just don't get a signal inside their establishments. The need to be reachable all the time is a relatively new one for the majority of people and we're obviously still experiencing some growing pains.

Dear *2600:*

This letter is in response to DJ Walker's letter in 24:2. First of all, I am a computer technician in a public school district. I have to say I was quite upset when I read your letter. It's not that computer technicians are incompetent. They are understaffed, underpaid, and controlled by incompetent superintendents.

Our budget for equipment is cut by 50 percent or more each year. Software is the same. We recently were approved for two more additional employees but because of personal grudges we are not permitted to start interviews yet. We are constantly hindered by our administrative staff as to how and when we are allowed to do our jobs. Now this being said, there are four of us in our department: three technicians and our systems admin. We support six buildings and are currently building another brand new shiny building. We support a 50-50 mix of PC (Windows XP) and Mac (10.4.10) clients with an 85 percent Windows Server (2000,2003) base. We have one technician, moi, who is certified in both Mac and Windows. (Guess who supports the MACs for the whole district along with doing all warranty work?) Our teachers all have district issued laptops and have no clue how to use them.

Teachers are extremely illiterate (unwilling to learn also) when it comes to computers and the administrators have the minds of cavemen. (How these people can hold doctorates and be this stupid is beyond me; it is amazing they can get dressed in the morning). Ninety percent of our tickets are for problems that involve stupidity. Was it plugged in? Did your battery have a full charge? Was it the right password? Did you spell your login name right? Were you plugged into our network or were you wireless?

You want to know why things aren't perfect? It's not because your techies don't know how to do it. They don't have the time or staffing to make it so. We were recently accused of "abusing the time clock" when we put in a combined 150 hours of OT just to get the district ready for the start of school. Your techies also most likely don't care. Don't get me wrong. A school district is a great jumping off point to a career but aside from benefits the pay sucks. Try living on 30k a year when you are married, have kids, and have a mortgage. The only people in a school district who get what they want are teachers. Unless you have a contract (or a union for that matter), you will be screwed in a school district.

On a side note, we are all open minded individuals in my department and 2600.com is not blocked in our district. We listen to all students who are willing to tell us if we are doing something wrong or if they found something they could get into that they shouldn't have. We don't punish curiosity.

Keep up the great work. Love the mag!

theforensicsguy

Dear *2600:*

In response to Guitarmaniax's comment in 24:2 regarding the "Redboxing in the New Age" article, I can say it's a relatively common phreak practice to refer to a telephone company by one of their older names when giving an explanation. In this case, I think it's being used to refer to the former SBC areas of AT&T territory. As some of the readers may know, BellSouth exited out of the payphone business in early 2001. If the author had simply referred to former SBC territory as AT&T, this could easily confuse someone who isn't too familiar with the telephone system in BellSouth territory. This isn't something that's native to Bell System territory, either. I'll try to not go into too much detail, but let's take Embarq, a telephone company that serves some of the more rural reaches of many states in the U.S. as an example. In Virginia, before they were known as Embarq, or even Sprint, the company that served the area was known as Central Telephone of Virginia. Exclusively in this area, test numbers such as an Automated Number Announcement Circuit, a machine that reads back the number you're calling from, as well as other fun things, are located in the 11x range, x being one through zero. Additionally, the code 959 and any last four digits in all of this area will take you out of the office you're dialing from and will reach a number on the nearest office to you that processes long distance calls owned by Sprint. In nearby Carolina Telephone territory, also owned by Embarq, both the codes 11x and 959 don't exist. Referring to telephone companies by their older names are just easy and unique ways of making clear who you're talking about (besides, I think "Central Telephone" sounds a lot better than "Embarq," don't you?).

ThoughtPhreaker

Dear *2600:*

"Less code and phone stuff." Seriously? C'mon,

this isn't the "Quilting Quarterly." I have to say over the years there have been many articles featuring code that was written in a language I was not familiar with, but to better understand the article I would learn at least enough to help me appreciate the finer points of the code. It has definitely expanded my horizons.

c0ld_phuz10n

In our recent survey, we received a lot of comments on both sides of this issue. At this stage it makes more sense for us to gravitate towards less code in the actual printed magazine with supplemental code available on our website. This allows for the pages here to be devoted to theories and explanations plus it also keeps people from having to retype or scan all of the code which can really be a pain in the ass.

Dear *2600:*

You have probably already received tons of responses to the article titled "Hacking *2600* Magazine Authors" by Agent Smith (24:3). I can only imagine that many people feel the same as I do about this article but I simply couldn't stay silent on this issue. Agent Smith should be very proud of himself for outing a coworker and probably getting him fired if not in serious trouble for writing about company system vulnerabilities. While I share Mr. Smith's sentiments about loyalty, as it is no doubt an admirable quality, what he fails to realize is that loyalty, like *respect*, is earned and not given blindly. One might argue that all employees should be loyal to the company for which they work. After all, they are employed of their own free will and can leave if they aren't happy with their job. That's all good and fine but the truth is there are hundreds of reasons someone would hold onto a job they don't like, not least of all fear of starving to death, fear of change and the unknown, and fear of leaving one's comfort zone. These aren't trivial matters for most people. I too work for a very large company with offices around the world whose name is very recognizable and I can speak from some experience on this subject. Large companies have a tendency to have a corporate culture that is not conducive to sharing information. Many companies don't even realize that they are doing this and sometimes they do it on purpose. The culture that you work in will determine how loyal, happy, dedicated, and hard working the company's employees are. It is almost as if the bigger the company, the worse the culture is for the employees. Many bosses do not even realize that they create and perpetuate an environment that encourages the behavior that the subject of your rant (the2600one) exhibited by publishing a seemingly anonymous letter in 2600. I'm sure Agent Smith is thinking, "Frankly I don't give a shit since I'm perfectly happy at my job and I'm treated with respect" but this may not be the case for someone who works in another department, in another branch, or even in the same department as yourself. Different units of the business may be run differently and may not have the same wonderful environment you, yourself, are subject to.

I can speak from experience when I say that I have seen bosses within my organization try to hush workers who expose vulnerabilities or simply try to improve horrible processes that hinder productivity and cause stress to the employees carrying out these absurd policies. In fact, many business processes are counterintuitive and just plain stupid. It sounds ridiculous but it is true. Is it possible that the2600one is not happy with his job because he has tried to point out vulnerabilities to his boss or coworkers and received a cold or indifferent response? Is it possible that this person is not happy with his job because the culture does not encourage intelligent thought and puts in place an environment which discourages free thinking and ingenuity? I would say it is very likely the case since most large companies want to do things the way they've always been done. They don't want to change, whether it is out of fear of the unknown, ego, or simply laziness.

The question I would ask is why an obviously intelligent person is not loyal to his company. You may say you don't give a hoot but if you care about your company so much you should care about this. It is likely that he is not the only employee in this situation and if that is the case you will see more and more articles in *2600* spotting holes in your company's infrastructure and systems. Which begs the question, why then, if you care so much about your company and are so loyal to it did you not report the article immediately to management and let them know that they have a major issue? Hmmm... looks like someone needs to think about what loyalty means while they point the finger at other staff members.

Logopolis

Dear *2600:*

I read the article on "Cheating" Goog411 in 24:3. One of the author's predictions is that Google will eventually pull the free connecting part, reason being "abuse" by people using it to connect to a variety of phone numbers that aren't Yellow Page type businesses such as payphones, ANAC, or loops. Far from it! In today's day and age, I'd even wager that a good number of wealthier *2600* readers might be willing to pick up the cost of providing numerous in-country phone calls, especially given the popularity of unlimited calling plans these days, just to grab onto a list of all the coolest or most popular and interesting phone numbers among *2600* readers in the country. Likewise, I'm sure Google uses the information the same way, to categorize how popular businesses are, and any sort of interference with that data collection activity would reduce the value of the project far more than the non-malicious playfulness suggested in the article.

Zaphraud

Dear *2600:*

Just read your editorial regarding the feedback you had been receiving on the subject of politics in your magazine. There are as many reasons to oppose political content as there are reasons to consume it, even if only in order to "keep your friends close, and keep your enemies closer." Pericles said "Just because you do not take an interest in politics, does not mean politics won't take an interest in you."

Like it or not, that world of politics is what ultimately decides which, if any, of our day-to-day actions makes us criminals, or what types of actions can be used against us as citizens. Those things should be of great interest to us all because they certainly affect us all. In my opinion, anyone turning a blind eye toward that has no room to complain when they don't like the result. I am not unreasonably concerned about *2600* losing focus due to any political content, and in fact I welcome it from a source unlikely to perpetuate the

mainstream media's ignorant bias.

Thanks guys, keep up the good work.

Dvnt

Dear *2600:*

I'd like to respond to the "Target: For Credit Card Fraud" from 24:3 with a bit of skepticism. First, I cannot see how he has done "more good than harm" by exposing this info about hacking into Target's internal network by not doing anything for "over a month" and then writing an article about how he illegally played around in it while he worked there and not show any evidence of reporting this security flaw to any Target authority. I am not trying to bash on *2600* for publishing it, but really, should these kind of articles get published?

I mean this guy is writing an article to a hacker mag a month after being an employee of that company reporting a flaw in their network and pretending to be a bad-ass, remaining anonymous, and pointing out how this information is only for advice to the company to change their security system.

He did not mention what position he held, but we can assume he did not have an authority position since he mentioned that he played around on the internal network from registers to computers in the employment kiosks along with managers' and backroom computers, therefore implying he was a ground worker without an office (therefore not part of the tech group) and that he did not do his job, but rather played around with people's information like a little kid writing amateur DOS batch files to retrieve this info.

A big concept that slipped my mind when I first skimmed through this article is that, if this kid knows all of this "techie" knowledge, why in the heck was he working at Target in the first place? Obviously this kid is either exaggerating or lying about the "break-in" he actually employed on the network. Discouragingly, this kid did not last long enough to explore the whole entire network. Oh golly! What a shame! He couldn't steal more credit card info or at least feel like he was stealing some valuable information that anyone can get access to. Come on, registers? In no way are they involved enough in the network to even have employee info. I've worked with registers in similar stores. You have no access to anything except a big calculator for retards.

In summary, this kid is either exaggerating on what he found or he is flat out lying. I've learned never to trust a source unless others can back it up and this is a good example of it.

Kid, I suggest you stop child's play and start doing what they pay you for and let the real techies worry about security breaches.

It just sickens me how anyone can write a BS article such as this and get it published. In no way is this article helpful to the readers, the mag, or Target for that matter. Don't wait a month to write a vague article on a company's poor security unless you report the flaw to the company first! If you don't, then you are indeed doing more harm than good, and shouldn't include the BS about "please do not use this info for malicious purposes." People like this make a bad name for hackers.

F33dy00

Do you really believe that there are no intelligent people working at Target who have "techie" knowledge? There are people everywhere who know things that may be a lot more than what's needed for their jobs. And regardless of whether or not this writer should have reported the information to his local supervisor before revealing it to the world, what's important is that the information wasn't kept secret. We've seen plenty of examples of how reporting something to your boss or teacher or even to someone you have no connection to can backfire and wind up causing you all sorts of problems. It's a microcosm of the hacker getting blamed for the vulnerability which he didn't create but merely exposed. And in this particular case, there are likely many other companies making the same mistake who will read this and learn something about what they're doing wrong - before it's too late. So while you may only see the evil that can come from disclosing such information, there is always a benefit to discussing these mistakes.

Incidentally, the system at Target may have been changed since this article was printed. In fact, we received this letter from the author of the piece after we had already put the article into the issue:

"I appreciate that you are going to publish my article, but I believe that by the time it is printed, the information will no longer be accurate. It has come to my attention that the deadline for PCI compliance is very close (http://www.pcicomplianceguide.org/). If Target is following the standards set forth by PCI compliance, then their security setup would have changed. I have no way to verify any changes have taken place, but I can only assume they have tightened up their security. I am requesting that you do not publish the article. I don't want to propagate false information and put the reputation of your magazine at risk."

Ideas

Dear *2600:*

The number of wireless connections in my 'hood is getting to the point where someone's connection overlaps someone else's. With that in mind I decided to make a political statement with my wireless router name by changing it from Linksys to IHateHillary (your statement here). Then my daughter suggested I change it to MoveYourTrailer so my neighbor would see it and move his trailer from right in front of my house. But what if I could communicate with neighbors using just my server name and the free transmitter it came with? I could change my server name to "are you there" and wait until a neighbor (i.e., neb) changes their server name to "Yes, #00X43", the data being some code word or anything you like. With a simple program, I could change the name of my transmitter and you could monitor changes to a name with a header and date field. Such as "Serv1-010110101011100" and you could respond with "Serv2-00011100101011010011". With a sequence number and data field, plus maybe some in band control bits, you could transmit all over. The only drawback is most Ethernet/IP connection software needs to reestablish the secure connection with a password every time the name changes. But this could be useful in an emergency.

FobG

Dear *2600:*

I'm a long time reader and recent subscriber (finally overcame that "being on a list" paranoia,

what can I say). Although I don't always agree with or highly value every single article, overall I really love what you guys are doing. I also take great pleasure in reminiscing "the good old days" while perusing some of the earlier issues. Some articles I even consider "required reading" and mercilessly harangue friends, family, and employees into reading them. It is this last concept that I wish to pursue further.

It would be amazingly cool (and more than a little useful) to be able to search your online index, find an article(s) or letter(s) of interest, and then click to go directly to the full text of the content in question. Even cooler if I could provide such access to my employees. Oh, I know that whole idea sort of directly threatens all you hold dear and sacred (i.e., your primary source of revenue) - but I'm not asking for free digital content. I already have the issues, I just want to be able to peruse them (and have my employees do so) - without thumb-printing them all up (hello, 23:4).

So, what do you think? I'd like to make online perusal of your magazine an employee benefit for my company, and I don't mind paying for the privilege. Make it an online service and I'll pay for subscriptions, or license it and I'll host it myself. Any chance in hell this idea goes anywhere?

thotpoizn

While it all sounds nifty, actually implementing such a thing requires a great deal of work and a lot of coordination. By no means is it impossible but we have yet to hear a plan that we're capable of implementing and that wouldn't put us out of business.

Dear *2600:*

Have you guys ever thought about maybe printing a reference book of the best printed and unprinted articles? Maybe classify them into pertinent sections according to coding, hardware, and useful programs. I find myself rifling through old copies of your mag for articles that I have read when I run into a situation and know that I read an article that has something relevant to the situation. I would love to add a *2600* reference style book to my desk at the public school I support and it would be great to index all of that useful info!

Matthew

This is something we're actively pursuing and expect to have more news about soon.

Problems

Dear *2600:*

Thanks for the great publication. I love it. I have been reading since I have been 12 and really enjoy it. I have had some problems lately that I think you great geeks can figure out or give some advice about. Here is my problem. I have been receiving a bunch of calls from the "Secret Service" lately and it is getting really old. I highly doubt that the Secret Service likes prank calling people, and I would like to know who is behind the problem. It is a private number which is the trouble. And I can't block all private calls because some of my friends have blocked Caller ID by default. So how should I go about stopping the calls and/or figure out who is calling me? I figure they are just from some other more immature 14-year-old not too different from myself. I am getting the calls on my cell phone which is the worst part. They call about six times a day and call between 3 pm and 11 pm.

Beachedwhale

Let's not be so quick to assume that the Secret Service doesn't like to prank call people. But you mention that this caller managed to block Caller ID which right there puts them at a level of sophistication beyond that of the Secret Service. So what you're dealing with is an entity who is calling you over and over again without identifying themselves. Back in the old days, this sort of thing happened all the time. Today it's so much easier to identify incoming calls even when they're blocked. There's no more running to the central office while trying to keep the caller on the line and taking 20 minutes to figure out what part of the country the call is coming from. These days it's all logged somewhere. If the Caller ID is blocked then you (the called party) simply aren't able to see that information. But your phone company can. Those are the people who can help you put a stop to this. There are other more tricky ways such as forwarding your line to a service that reads the ANI data rather than the Caller ID data. A few years ago a company named Z-Tel inadvertently provided this service to their customers when forwarding calls to another line. Someone could call your landline with their Caller ID data blocked, the Z-Tel service would ring your line and after a certain number of rings would forward the call to a second number that you had designated as part of a "follow-me" service, and the caller's actual number would appear as the incoming number on the second phone regardless of blocking status. This little feature was discovered and "fixed." But there are undoubtedly other ways of doing this and we're sure our readers will send in suggestions. For now, simply don't pick up blocked calls and return the phone calls of anyone you know who calls you with their number blocked. When the people behind this stop getting anything other than your voicemail, they will grow bored and move on to something else like physically attacking you. And then you'll know who they are.

Dear *2600:*

Although this letter has nothing to do with phreaking or technical hacking, it entails an interesting situation about socially "hacking" the educational system:

The high school which I attend uses the Prentice Hall biology curriculum for their biology courses offered through the International Baccalaureate program. It turns out that this is the exact same curriculum that I used in middle school through a "gifted and talented" program in seventh grade. Upon learning this I was incredibly disappointed. After all, I would not be learning anything new in one of my favorite subjects for an entire semester! Then it dawned on me: besides just having remembered all of the information within the textbook, I still had a copy of every single test and assignment for that textbook. These are the standard tests devised by Prentice Hall Publishing, mind you. In the IB program and in my high school, it is considered academic dishonesty or "cheating" if one somehow has a copy of a test prior to the administration of that test, hence the solution to my problem. If I tell the biology teacher and/or the IB administrator that I have these and submit copies to them to prove it, they may bump me up a semester to material I haven't learned yet! I could say that it wouldn't feel right on my conscience to cheat in this

manner, that I fear penalties, etc. The obvious pitfalls to this approach are that they could just give me alternate, and undoubtedly easier, tests, or they could use tests different from the standard. There is also the possibility that they would just not care or that they would confiscate the tests. (I will make copies which I won't turn in.) I have been lucky so far, compared to many hackers, as to the quality of my education, and I am worried somewhat that my luck may run out and the teachers will resort to ludicrous measures out of laziness. If they state that I couldn't have remembered all of that, then they would be condemning their own teaching methods. How do they expect us to recall it in real life, then? Plus, there is still the fact that I will be bored, having learned all of this previously. Thus, it is a fairly positive situation for me either way - they either move me up in the curriculum or I get an easy A, the latter being the less desirable of the two outcomes. The true colors of the IB program and of my high school, which is highly touted for a public school, shall be revealed regardless. Needless to say, it will be interesting to see what comes of this. The things one has to do to learn....

The Philosopher

Dear *2600:*

I have a story for you but it's not about hacking. My wife and I were visiting family and staying at an unnamed motel. This motel was one of those really cheap ones where you go for affairs and stuff. Anyway, this hotel advertised Free Wireless Internet, which is one of the reasons I chose it. I was browsing around the Internet using their network when I got curious. I wondered what type of router they were using and how secure it was. So I opened up the command prompt, got the IP address, and typed it into the URL bar. A familiar screen popped up. It was the same one from my wireless network at home. So I knew they were using a Linksys router. Then came the admin name and password prompt. I thought I'd give it a shot and use the default which is no admin name and the password is "admin". I mean, no motel, hotel, or any other place would be dumb enough to leave it as the default settings but I figured it wouldn't hurt to try. Lo and behold I was granted access and the all too familiar, to me anyways, configuration page popped up. It was so easy to get in I was stunned. I looked up in the upper right hand corner of the screen and noticed they were using the same router I used at home. At this point I could have changed whatever I wanted but I didn't. I didn't bother telling the guy at the front desk because he would have blown me off and he probably would have called the cops and said I was hacking into their network. I thought I would share this story with you to show how some people still don't care about their network security.

Togeta

This is primarily because most people aren't network admins. Odds are the guy at the front desk has no skill or interest in this department at all and his solution to the problem would be to just unplug the thing. While large chains can afford to hire IT guys and ensure that routers don't get installed with default passwords, the smaller places might wind up not offering the service at all if it becomes too problematic. That's why education on a very basic level is so important. Something like this should be as intuitive as locking a door.

Dear *2600:*

I don't know why, but the last two times I've purchased *2600* at my local Borders, they have been unable to scan the UPC and get it to ring up. They will key it in manually as a generic periodical, which as far as I know means you guys don't get any sort of credit or anything for it. Just a heads up.

Ramie

Borders doesn't have this policy but Barnes and Noble does, where issues that they lose track of get charged to us. Thanks to you and the many others who are keeping us updated.

Dear *2600:*

I work at a college in New Jersey. To put things into perspective: The people who run this place think that technology means more computers in the classroom We recently switched from a Novell server (which was seven years old) to a Windows Active Directory server (which is new). So the guys from the IT department installed WAD on my machine. I asked the IT guy, "Do I keep the same password?" His reply was, "No, here's your new password." He then told me that my username was "jsmith" and my password was "js1234". "1234" is my phone extension on campus. How secure is my (or anyone else's) password and files if everyone knows how to get in? Luckily I was able to have my IT guy change my password so no one knows what it is.

Since everyone's password is not protected, can I log in as the college president? What about the head of the IT department? Facilities? Finance? I haven't tried it, but I'm very tempted to.

hypo

What's even more amazing is that you apparently don't have the ability to control your own password. Giving out a default is fairly standard and not necessarily insecure if it's followed up immediately by a password change. This apparent missing second step at your institution is indeed a major problem.

Dear *2600:*

Please stop all subscriptions addressed to the facility listed above. This is a state hospital for civilly committed sexually psychopathic personalities and sexually dangerous persons. It is inappropriate for them to receive this subscription. Your publication jeopardizes the security of our facility and places a risk to patients, staff, and the public.

Office of Special Investigations

We've been accused of a lot of things but jeopardizing the security of a civilly committed sexually psychopathic personality is a first. We're also not sure how such a person reading our magazine puts the public at risk but we'll defer to your judgment on that. However, as the person(s) who subscribed to us at this institution paid us for it, we must notify them and issue refunds for the unreceived issues. Hopefully that won't cause more grief.

Questions

Dear *2600:*

Are you interested in an article about spoofing fingerprint biometric sensors? I've just done a bunch of work on fake fingerprints and I could write a pretty nice how to (actually addressing the practical issues

and what the best methods are, unlike most of the academic world). I've also got some stuff on Albert Wehde, who seems to have been the first guy to forge prints, way back in 1927 when he was in federal prison for gunrunning.

I'm asking instead of submitting because I haven't read *2600* for a while and I don't know if you want to cover this stuff or even if you've covered it recently. If you're interested, what sort of word count do you usually want?

M

Anything involving spoofing, bypassing security, or just plain mischief is most certainly something we'd be interested in hearing more about. As for word count, just shoot for long enough to tell your story as thoroughly as possible without becoming boring.

Dear *2600*:

After getting a hang up on my phone showing a number of 214-000, I started Googling and found out that maybe 214-000 has something to do with calls coming across from Mexico via Texas. I then stumbled across some postings about this number: 214-586-0999. When I dial it a synthesized voice called out my phone number then said "Please wait while I connect your call." I then get some interesting new-agey techno music that just goes on and on. Anyone know what these numbers actually are?

Doda

This number is indeed interesting. While we couldn't get it to read out the phone number, the endless musical hold is apparently unavoidable. Judging from the many comments about the number on the Internet, it seems to show up on various calls from other countries all over the world. There is wide speculation that this is some sort of a VoIP service where the phone number is being manipulated. We'll keep our readers updated if we get any more info.

Dear *2600*:

Not sure if this is possible, but could you get me in contact with the writer of an article in the current issue? The reason for my interest is that I was intrigued by their analysis of the network and I work as an engineer for a competing company. So I am interested in what we can do to secure our product.

David

If a writer wants to be contacted, he/she will add an email address to their byline. Otherwise we have to assume they don't wish to receive correspondence. And we simply cannot serve as a go-between for a whole variety of reasons.

Dear *2600*:

I received this email as the date indicates and I was wondering if this can be traced to the sender or an origin? I should have written sooner about this. I was reading the article "Hacking *2600* Magazine Authors" in 24:3 and it got me to thinking about this threatening email I received back in April of this year. I have treated this as a prank mostly except I did have a short connection with the FBI when I was asked to do some radio monitoring after I tuned in a strange radio transmission in CW I intercepted off of the 30 meter ham band.

I buy *2600* off of the mag rack at Hastings regularly and appreciate the work all of you do. So thanks for reading this and be careful out there!

----- Original Message -----
Sent: Monday, April 16, 2007 12:58 PM
Subject: Comply with us or you die

Do you want to live? Comply with us, even as you reading this mail, you are being watched. Your internet and telephone are tapped by us. This is a serious case. After, reading this mail, don't try anything stupid. Don't involve police, interpol, or FBI.

I am a strong member of islamic shite and an assasian by profession. I am from Afghanistan. I was paid by someone to assasinate you and your family by bomb blast last weekend. We have carefully monitored your family for one month now and we have your family profile and personal data.

You are supposed to be a dead person by now, but we want to give you chance to live if you comply with us by doing what we will ask you to do. Your family cannot run or hide from us because we have network almost all over the world. Remember , we are watching now and if you involve police, you will die!!!

May Allah be blessed.

John

In a way this sort of thing was inevitable. The old style spam of simply trying to con people out of their money may well evolve into outright threats and intimidation tactics to extort people. We find the letter extremely humorous but you undoubtedly don't. Our unprofessional opinion tells us that the level of absurdity contained within indicates that this thing isn't for real. The fact that they mention the FBI and that you already have been involved with the FBI leads us to suspect this is someone who knows this about you. And if somehow this information went out over one of the ham bands, then that is almost certainly what is happening. There are all sorts of ways of figuring out where the mail came from based on full headers (which weren't forwarded to us), the appearance of the email address in public posts, and other clues. But it's also possible to mask all of this information with a tiny degree of competence. Then you must look for other clues within the body of the message, the timing of its delivery, etc. And if after all of this you find that it's keeping you up at night, by all means contact someone in authority who's capable of understanding what's going on. Threats of violence should never be tolerated.

Dear *2600*:

I've been enjoying *2600* for some time now and would like to have your voice around for a lot longer. To that end I've often wondered which method of buying the magazine is most beneficial to you guys. For example, do you need sales from my local bookstore to increase circulation through distributors and make it worth giving you shelf space? Or do you prefer the extra money you get from subscriptions? Does the discount for multi-year subscriptions really outweigh the cost of renewal notices? It seems like lifetime subscriptions give you cash up front, but do you then regret it when subscribers live forever?

In short, assuming minor price differences and paranoia about subscribing aren't a concern to me, what way of buying the magazine does the most to keep *2600* viable in the long run?

RB in SF

The only real answer to this is to recommend that you do whatever is most convenient for you and that

you keep doing it. If you subscribe and forget to renew then obviously that doesn't help us. And if you keep going to your store in hopes of finding us and either get there too late or aren't lucky enough to have a store that carries us in your town, then subscribing helps both you and us. We hope people find us in bookstores and don't just bring issues over to the coffee section and get stains on them. While it's good to see stacks of issues in stores, if they remain there for too long it becomes a problem. It is your civic duty to see that the issues get sold to people who can appreciate them. We're not asking that you drag total strangers in off the street and demand that they buy an issue (although we're not forbidding that action either) nor are we suggesting that you buy all of the issues yourself and then hand them out as gifts and swallow the loss without complaining. What we would like is for people to be aware when a new issue is out and for them to alert others so that our sales do well and we have enough to put out the next one. Our readers have always been very loyal and, as we're 100 percent reader supported, they are literally the only reason we're still around. If we were advertiser supported, the numbers could be fudged in order to keep the advertisers paying whatever we wanted, resulting in a publication that served no one but ourselves. That, unfortunately, is a common practice and it's one of the reasons we've resisted even cautious steps into that world. So please subscribe or buy individual copies in whatever manner is best for you. (No, we don't mind when our lifetime subscribers live forever.) In short, spreading the word always helps. But thanks so much just for caring enough to ask.

Dear *2600:*

I've been an avid reader of your publication for several years now and I love the technical information presented. I do have a question for y'all, however, which deals with capturing streaming video as it appears on the PC. On youtube.com, there are several videos which take a while to download. It would be great if it were possible to record the streams to a file on the hard drive so it could be watched later without the continued pausing which occurs when the additional video has to be downloaded.

What I have tried already is to right-click on the page that is playing the stream, select View Source, and then save it to a ".txt" file. I then opened the .txt file in Notepad.exe and performed a search for links that ended in the standard suffix associated with video files (i.e., .wmv, .swf., .asp, etc.). On the rare occasion that I found one, I would cut and paste it into my browser's "www" field and click go. However, this did not appear to work.

Is there any other method by which I could capture the streams?

CMG

Yeah, there are methods that actually work. One you might want to try is YouTube Downloader which can be found at http://youtubedownload.altervista.org/.

Dear *2600:*

Hey guys. Are you interested in Polish payphones? Well, if you are I could take some photos. Just tell me.

suN8Hclf

While this somehow feels like we're entering into a drug deal, yes, we are interested. Hook us up. Thanks.

Dear *2600:*

Any chance of you guys doing an article on the Sidekick?

BiomechanoidXIII

Only if someone writes one. Our address is articles@2600.com.

Dear *2600:*

I just got done reading 24:2 and found it to be very well informed. I truly enjoyed reading it although this edition was my first and only issue. I don't have access to a computer but I plan to remedy that in the near future. In the meantime I was wondering if you could provide me and/or direct me to any information regarding the following:

1) E Door Tracker.
2) ATM Technology (i.e., keypad, etc., etc.)
3) Websites that contain hacker equipment.

In closing I thank you in advance.

Anthony

We probably shouldn't ask what you're up to but all of what you seek can be found on the net just by plugging those phrases (and others) into a search engine. There's way too much to simply provide to you while you don't have computer access and we're not sure what good the websites would do you during that time anyway. We suggest having a friend print out a bunch of stuff from some of the results of this search. It will keep you busy.

Dear *2600:*

How does one catch someone who is backspoofing the telephones at home and the cell phone? I know it is happening but I don't know how to find out who is doing it.

Christine

We'd be more interested in hearing how you "know" this is happening. We get letters like this all the time where people are convinced someone is watching their every move or impersonating them but without a clear picture as to just how this conclusion was reached, it's impossible to give good advice. Spoofing Caller ID isn't very hard to do which is why nobody should rely on that data for any sort of identity verification. It would be a good idea to not use any service that does.

Dear *2600:*

What's the deal with the Winter 2006-2007 cover? Why is Bob Dylan shaking hands with the guy from the "Take on Me" video by A-Ha (80s band)? What's in the suitcase? Why in front of the Merrill Lynch bull?

W1f3y 0f R34d3r

It represents the joining of forces to prevent Merrill Lynch from moving uptown and destroying the Hotel Pennsylvania. We just didn't know it at the time.

Dear *2600:*

Do you have any surveys which show the most popular computer companies? Under each company what is the most popular computer? What is the most popular OS? Who has the best customer service? Do you have anyone who can write a program starting

with DEBUG? Do you have anyone who does assembly language programming on a DOS/Windows OS? If so, what books does he recommend to help me learn this language?

FK

Do you ever write anything that isn't a question? Most of what you're asking has nothing to do with our subject matter, is way too general, and is really stuff that you get to learn on your own after playing around with computers for a while. You will find plenty of people willing to give you advice once you get involved.

Surprised?

Dear *2600*:

I just picked up your latest zine (24:3) at the local Barnes and Noble which displays it right out in front of all of the other zines. I noticed the white blocks on the outside binding and remembered seeing them on a couple of past issues. Well, being home alone bored I thought of putting the issues with the white blocks together in a stack to see if the blocks would fit together and maybe see some kind of message. After several tries I finally did see something. It looks like the letters S-U-R-P-R-I-S-E and then something that looks like a B or maybe an 8 and lastly maybe a symbol of some sort. I see this when I stack them: 24:2 on top, 24:3 in the middle, and 24:1 on the bottom. Please tell me if this is something or am I seeing things? If it is something I guess I'll have to wait for 24:4 to see what the last two things are.... Or will I?

SJKJRX

Stacking issues out of order - what is this world coming to?

Dear *2600*:

Is "surprised?" the final message on the spine of the last three issues, or is there more?

MasterChen

What do we get if we answer correctly?

Dear *2600*:

OK, so ever since I read one letter that was sent in saying that the writer was only trying to get his name in the magazine, I was intrigued. But I also realized that if everyone did that, then 1) there would be an issue and 2) it could be considered spamming *2600* (which would be interesting) and would raise the already enormous letters section to a really huge size.

So there really is a point to this letter. I see that there is an interesting factor to your new binding of the magazine. And in a future response to your question: no, I am not surprised. Hate to disappoint! Keep up the great articles!

PreisT

Dear *2600*:

I have noticed your spine on the new *2600* mags. If I place them in order of 1,3,2 it seems to say Surprise07. I think the last issue of the year will be the bottom so the order will be 4,1,3,2. Does the order of the mags mean anything?

I know a lot of the readers don't like the new spine. But I do. Center pages and back cover do not pop off after heavy use now. So it seems to hold up better.

Keep up the good work. And hidden treats.

Unknown One

Dear *2600*:

"Surprised?" That it was that easy? Yeah, I kinda am.

stranger0nfire

How about the fact that it wasn't supposed to be completely readable for another year? Perhaps it should be changed to "Shocked?" for our benefit.

Opportunity

Dear *2600*:

Good Day!

Barrister John Ibe is my name and a Senior Advocate of Nigeria. I have a proposal to discuss with you concerning one of our Deceased customers who is a national of your country. As soon as I hear from you and once we are in agreements. I would be needing your assistance in making a business investment in real estate, oil & gas and any other lucrative sphere of business in your country.

Owing to the urgency of this transaction, I would appreciate an immediate response from you to confirm the receipt of my mail. As soon as I get this response from you, I will furnish you with details of the transaction and the urgency at which I need to get the funds transfered out of Nigeria to you. Your earliest response to this letter will be appreciated.

John(SAN)

We really want to do business with you but feel uneasy because of the grammar and capitalization issues we've previously written to you about. One of your colleagues even sent us a letter that was completely in capital letters! We simply cannot abide that as it makes us feel quite small in comparison. Once we have the protocol sorted out, we would be most happy to supply you with all of the information you need and more in order that we may help to secure the transfer of the funds from Nigeria. It is indeed disturbing how much money has been tied up in your country over the years simply because there aren't enough people in the world who can give out their bank account numbers and transfer codes. Please count us in as concerned parties who want to help. Yours truly, etc.

Observations

Dear *2600*:

I really enjoy your publication. Although I'm not a "hacker" myself, I feel that I'm much more enlightened concerning computers in general because of your efforts and publication. Great job. Thanks and keep up the good work!

Now that that's out of the way, here's something that perhaps a good hacker could tackle. A couple of years ago, my wife bought an HP 8250 "Photosmart" printer. For the first time, a few days ago, I got into some of the more esoteric areas of its control panel, and wow, there's a lot of information there. One of the things that caught my eye is the "expiration date" of the ink cartridges, which I take to indicate that you have to buy a new one from HP - because it won't use the "expired" one whether it has ink or not. A clever

way to keep the revenue stream up, huh?

Why doesn't someone poke around with these things and see what you can learn? If the ink cartridge has a chip that can be flashed, then cartridges could last - well, essentially forever!

If you've already written about this, I'd be grateful for a reference!

PlumBob

We've never heard of a printer refusing to use an ink cartridge because of a passed expiration date. You may get an annoying popup message and perhaps a dire warning of a voided warranty should something go wrong but that's about the extent of it. Any company with any sense would know that this kind of forced control over its customers will simply stir up bitter resentment against them, not to mention all sorts of ways to bypass their restrictions.

Dear *2600:*

After more than seven years of reading I finally subscribed to the mag... and it felt good. I also just renewed my WBAI membership during "Off The Hook" and it also felt good.

In my stroll down memory lane I picked up the Winter 2000 issue of *2600* and in the "Direction" article you say something that still rings true today, "Their (music industry's) lack of foresight is overshadowed only by their naive insistence of using bullying tactics to get their way and hold onto that which was never theirs to begin with."

After the recent $220,000 ruling against a poor woman who downloaded (allegedly) a little over 20 songs, it makes me think that in seven years the RIAA still thinks that bullying works. It's too bad more people don't read, subscribe, and support your efforts because then maybe the bullying would stop.

Stay Human.

hypoboxer

Bullies only go away when people stand up to them. It's worth the occasional black eye if some other eyes get opened as a result. Oftentimes just making others aware of what's going on is enough to start changing the situation. And there's no doubt that this particular situation is changing.

Dear *2600:*

One day after returning home from work, I was surprised to see a package addressed to me from a total stranger. Anticipating a puff of anthrax, I opened it up to see my autumn issue of *2600* along with a letter. Apparently, my copy of the magazine got stuck to that of another subscriber and both were delivered to his address. But instead of throwing it away and just forgetting about it, he went totally out of his way to mail me my issue. I just want to express a public word of thanks.

Mike
Alexandria, VA

This is indeed the true spirit of 2600 readers and we also thank Ed for his consideration. Now we intend to figure out how in hell some of our envelopes are sticking together. Thanks for letting us know.

Dear *2600:*

Imagine my delight to learn that a lifetime subscription costs so little. Imagine my horror when I bought it and started receiving advertising addressed to my *2600*-specific nom de plume. American Express, no less. Gee thanks, *2600*, for killing trees in a vain attempt to sell me credit card that I already carry even.

Has *2600* sold out? Is all lost? Is the end near? Repent, and sin no more, oh corporate shills, and remove my address from your hounds-of-mail.

DataBoy

We've done a thorough investigation into this and we've been in touch with you over it as well. We don't know how American Express got your info but we can say that it most definitely wasn't from us. We take this sort of thing very seriously and go to great lengths to make sure our subscribers retain their privacy. But we don't for one minute think that there aren't forces out there working to somehow subvert this system which is why it's so important to always be alert and aware of any weirdness going on. By all means make a slightly different name or address for your subscription, not just for us but for everyone you give your address to, so that you can see who's giving your information to whom. The only possible way your address could have been passed along from when you placed your order was if someone manually copied it down at the post office or if somehow PayPal (where your order was placed) harvested it when you entered your information. If it's the latter then we undoubtedly will be hearing more about it, not only from our readers but from scores of others who use their service.

Dear *2600:*

I've been a reader of *2600* since about 1998 so first let me say thanks for giving me something to look forward to every three months. I also catch *Off The Hook* and *Off The Wall*, although mostly webcasts these days as sadly I've moved off Long Island.

Anyway, I just thought you might get a kick out of this website - in particular, the user agreement which can be found here: http://www.cybertriallawyer.com/user-agreement

Towards the middle you will find my personal favorite snippet: "*We also own all of the code, including the HTML code, and all content. As you may know, you can view the HTML code with a standard browser. We do not permit you to view such code since we consider it to be our intellectual property protected by the copyright laws. You are therefore not authorized to do so.*"

I am just curious to see your opinion of it, as well as the opinion of the listeners and viewers. Keep up the great work and rest assured you have a loyal reader/listener for life.

speedk0re

This is just so typical of the corporate world and how their little fantasyland becomes reality on so many levels. We live in a land where filmmakers have to cover up ads in public places or blot out the names of products or logos on t-shirts because they haven't gotten "permission" to use these images. Groups of people who sing "Happy Birthday" face prosecution if they don't pay for the rights. There are even those who believe you can be prosecuted for taking a picture of a building without getting the permission of the people who "own" the rights to its image. And now a website that tells you that you are not authorized to read its contents. Since we have now printed their words without getting specific permission from them, we can only cower in fear in anticipation of the action that will undoubtedly be taken against us.

What a screwed up planet we have become.

Dear *2600:*

I was recently returning home from overseas on a Lufthansa flight. It was one of those planes where everyone has their own personal TV at their seat and you can choose what movies/TV shows to watch and they start on-demand. Quite a number of airlines have these now for long-haul flights. It's pretty good - you have a selection of several dozen movies and a bunch of other crap too. So anyway, I'm not sure what I did but I managed to "crash" the console so that it just kept resetting to the main screen no matter what I selected. I called the attendant over and he had his colleague reboot the unit (somewhere out of sight from my seat).

This is when it got interesting. On the screen, I saw what looked like a DOS boot screen! Unfortunately I did not copy it all down in time, but it started like so:

Windows CE Loader v2.7

Part #...

It loaded a file called epos9.bin or something like that and mentioned a company called Rockwell. It also listed a server IP of 172.18.22.18 and a terminal IP of 172.18.22.20. I think these are internal local reserved IPs like the more common 192.168.*. It also did some TFTP transfers of the system files from the server and I'm not sure but I think I saw something about X-modem(!) mentioned too. Anyway, soon after all this interesting data, the graphical screen loaded up and I was back into the normal mode of the device.

I thought it would be interesting if anyone knew more about how these worked to share with the rest of us. Are they just glorified PocketPC MPEG players? Could any interesting effects be achieved by "hacking" these? For example, uploading your own videos to then show up on people's TVs? The possibilities are endless! To see the info firsthand, just act dumb and tell a flight attendant your TV isn't responding and ask them to reboot it for you. Then have a pen and paper ready!

Brian the Fist

A lifetime subscription to anyone who adds "Freedom Downtime" to their plane's collection of films. (If you wind up screwing up the navigation system this offer is void.)

Dear *2600:*

I was reading up on Edgar Allen Poe on Wikipedia and read about the Poe Toaster. The description they gave on the site sounded very similar to a scene in Freedom Downtime. So I think this mystery dating back to 1949 has finally been solved.

drlecter

It sort of flies in the face of the time travel theory presented a few pages back but we're certain there must be some rational explanation that we're incapable of grasping.

Dear *2600:*

Apple has such a unique way of working the system, especially the media. They make their products look nice and pretty, along with making them seem sophisticated but simple to use, so it appeals to the more clueless individuals. Then Apple calls in the news media to announce their product launches, while at the same time they pay TV and movie writers to work Apple products into their productions. This way, many people see the product and say "Ooh! That's hot! I have to get one of those!" And before you know it, everyone is talking about it. This concept is very similar to how the sports car manufacturers like Ferrari and Corvette have so many people thinking that a big, expensive sports car is the ultimate thing to have. I think that Apple's iPhone should be more accurately labeled as the "product hype of the year."

Jeff

Dear *2600:*

Regarding Ian 2.0's comment in 24:2, pages 44 and 45, I am generally in agreement with him. As is my tradition, I read 2600's summer edition lying in a hammock in Algonquin Park as part of my vacation reading.

The pattern that my wife and I follow is to take August off and to be offline for three weeks so we can go camping, get outside, and be active. I can't stress enough how valuable this "offline time" is and that I can't recommend doing it more. It serves as time to clear one's mind, reflect, relax, and see the offline world.

Thanks for the great magazine all these years. Tomorrow I head back online. Today I write postcards while enjoying the human scenery of the coffee shop.

Boomer/NTT

You have indeed made us jealous. You might want to consider one of the semiannual European hacker camps which is a good mix between being online and being in the wilderness. Of course if you really want to get away from computers, it might drive you mad.

Dear *2600:*

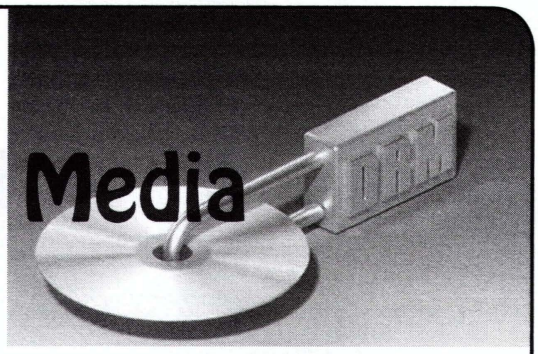
I recently stumbled headfirst into your publication and radio adventures. I was doing research on DeCSS for a paper that I was submitting to the Free Software Foundation and I came across the audio recordings of Emmanuel's deposition. Ever since then, I have not been able to quell my need to read and listen to as much information coming from *2600* as possible. I have been buying the magazine and listening to the radio archives for almost a year now. Of course, *2600* has merely been a jumping off point. There is never an issue or a radio show that goes by that I don't hear of something new to research or investigate.

I have been a hacker for over 20 years. I just never knew that there was this culture of individuals that thought and felt the same way about technology. Most of the technologists that I have worked with and met over the years have been "go with the grain" sort of people. I don't value going with the crowd merely for the sake of going with the crowd. I just wanted to take this opportunity to thank you for your great endeavors over the years so that individuals such as myself could have an outlet and a community. I have been inspired to start a *2600* meeting here in West Virginia. I will send you all of the details when things get off the ground.

Matt

It's always good to hear from people who have been affected by our world somehow and, better still, have been inspired to do something of their own.

Hacking Windows Media



by Alt229

Like vegetables being thrust into the face of an unsuspecting child, I was recently pushed into the middle of the Digital Rights Management debate. I wish I could say that I was doing something as noble as recreating *Star Wars* in ASCII format, hacking Microsoft, or leveling up my level 36 night elf druid. No, I was doing nothing of the sort when I got a first-hand taste of DRM. I was looking for naked girls.

My "research" started last month while my girlfriend was out of town for the third week in a row and I'd grown seriously tired of the same drunken college girls making out on the same couch with same drunken frat boys watching. It seemed like I'd seen everything on the net when I happened to stumble across a site that allowed unlimited downloads of their DVDs for only $30 a month. Unlimited downloads? I'd never paid for porn online and hadn't bought printed porn since I was 18, but this seemed like a good deal, so I signed up. Little did I know, but these guys used some serious DRM.

Here's what you should know about the possibilities of Windows Media DRM:

You have to type in your username and password into Windows Media Player every time that you play a video.

You have to be online so that Windows Media Player can connect with the licensing server.

You can only play the videos in the Windows version of Windows Media Player. Macintosh and Linux are not supported.

You will be unable to play any files you've previously downloaded once your account is deleted from the licensing server.

Of course, I didn't learn of these philistine restrictions until after I'd handed over the money, but after I did, the hacker in me knew that there must be a way to unlock these files. The following is a guide to decoding Windows Media DRM protected video files.

In order to decrypt a Windows Media DRM file, you first need to have rightful access to the file in question. If you don't know the username and password to play the file, you won't be able to decrypt it with the tools here. You also need a computer capable of running Windows Media Player in debug mode and copies of two decoding tools named drm2wmv and drmdbg to decrypt the data.

Before we get into decrypting a WMV file, let's look at how Windows Media DRM works. Each WMV file with DRM has two keys associated with it. One is called a KID and is basically a public key that identifies the file. The other is the SID, which acts more like a private key. You'll need both of these to play the file but the hard one to get is the SID. It's the protected private key that, if in the wrong hands, allows the user to do just about anything to the encrypted content. The secret to getting this key is to use a little known feature of Windows Media Player: debug mode. While Windows Media Player is in debug mode, other programs can access variables that are normally hidden away from prying eyes. The newest Windows Media Player as of this writing is version 10.00.00.3990, which will not work for our purposes. Microsoft realized that debug mode was the proverbial weak link in the DRM chain so they disabled the use of it when playing a file which is DRM enabled. The latest version of Windows Media Player that I've seen working is version 9.000.000.3344. It should be noted that if you've ever installed WMP10 and then revert back to WMP9, this hack will not work.

Now, let's get to implementing the hack. First, I recommend starting with a fresh copy of Windows XP. You **can** do this without having a clean install, but there are various DLLs that need to be a specific version for our little scheme to work properly. Some graphics and video programs will overwrite these files we depend on, and this will prohibit us from stripping the DRM. Again, updating to WMP10 will ruin your decrypting efforts.

So, assuming you've got a clean XP install and Windows Media Player 9, we can continue. First, make sure that you can actually play the video you're trying to decrypt. If you can't play the file, then you need to troubleshoot why; our tools will not work until the video plays properly. There was one DRM-related update I had to run for WMP9 to get the video file working in the first place. Running the update that allowed me to play the video didn't impair my ability to decrypt the file later. You may have to do the same.

The next step in our decoding process is to get the decoding tools. There are two programs we'll need. One is called drmdbg, which opens Windows Media Player in debug mode and extracts the SID. The other program, which is called drm2wmv, decrypts the WMV file with the SID from drmdbg. There are different versions of both of these programs, and different versions will work better in different situations. There are two versions of drm2wmv. One is written in Japanese and has cryptic error messages; the other, drm2wmv_e, is translated into English and has

more sensible error messages. I recommend the English version as it worked much better for me. As far as drmdbg goes, there are three versions that I've found: drmdbg-031, drmdbg-527, and drmdbg-621. They all extract the SID from the WMV file, but I've had the best luck with version 527. Normally, you have to scour Winny, Ares, or Gnutella for these files, but I've made an archive of all three versions of drmdbg and and both versions of drm2wmv to make your life easier. You can find the archive at `http://www.megaupload.com/?d=5O14MCK2`

Once you get and extract this file, you'll notice a bunch of different files and folders. We'll get to those in a bit. For now, just run any version of drmdbg. It will open up Windows Media Player and wait. This is when you should open up your protected video file. The player should contact the licensing server as usual, but then it should quit, and you should see a message saying that the KID and SID were copied to the clipboard. If the file doesn't play or if the file just plays normally, then drmdbg is having trouble getting the SID. Try using a different version of drmdbg. If none of the versions you have work, check for a newer version online, or install VMware and get a clean install of XP to work with.

Once the SID is copied to the clipboard, you need to put it into a file in the `drm2` folder. The name of the file you create doesn't matter, but the extension has to be `.key`. We'll call the file `nodrm.key` in our example. So, make the `nodrm.key` file and paste the contents of the clipboard into it. A sample key follows:

```
<DRM2WMV2>
<KID>oxQ+ql0iWEGMTEHW9U6erQ==</KID>
<SID>tD6TrfMAnMgeIzQ1eWVlGEODHGs=</SID>
<INFO>Z:\Movies\Pr0n\video_
➥with_drm.wmv </INFO>
</DRM2WMV2>
```

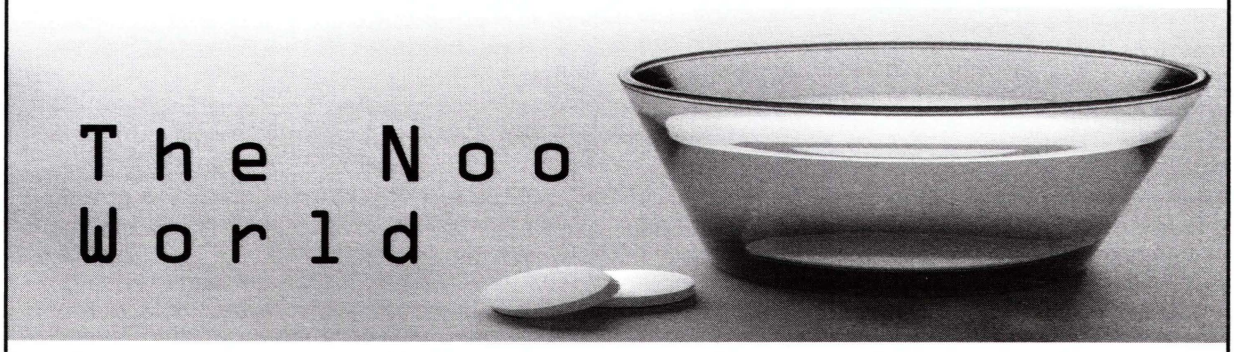
When you paste the key, it will all be on one long line and contain weird carriage returns. I replaced those strange characters with actual carriage returns here but you don't have to worry about doing so yourself; the program will work fine with the badly formatted text as it is. You can also place multiple keys into one file; just place each of them on a new line. Now save the file.

Now it's time to run the main decrypting tool, drm2wmv. This part, if you've made it this far, is the easiest. Simply run the drm2wmv command on the file you want to decrypt. In our example, this will look like this: `drm2wmv_e Z:\Movies\Pr0n\video_with_drm.wmv`

You should then see a progress bar move across the screen, and a new file will be created called `[nodrm]-video_with_drm.wmv`. Notice that when you open the new file, it won't run through any of the authentication techniques and the file is now playable on a Mac! Sweet!

This isn't the only way to unlock a DRM-protected WMV file. There is a graphical tool that attempts to decrypt these files (which is included in the zip file) more seamlessly, but it didn't work all of the time for me. Also, there are, and always will be, tools that record the raw output of the media player, but since we lose a generation, I chose not to use this method here.

Thanks! And happy downloading!



The Noo World

by Agent5

This article is intended as a resource to assist the reader in understanding a topic not heavily understood as of yet. Every person is different and every situation is different. The information provided here is offered as a possible answer to many potential questions. The author is not responsible in any way for any consequence resulting from reading this article.

So, suppose you're googling around cyberspace, letting your ADD run wild, looking up any interesting words or subjects you may happen to come across. You have every subject from aXXo to Zen Computing in a tab in your browser. Then, you come across a word that has a nice "cyber" sort of ring to it: "Nootropics". (Ah, Boredom, the places you take me sometimes!)

Nootropics are a new type of drug. They were originally designed to treat such neurological disorders as Alzheimer's, Parkinson's disease, and ADD/ADHD. However, recent studies have produced results which suggest the use of Nootropics by healthy people.

Imagine, if you will, a pill that makes you more focused, helps you form memories better, or lets you stay up for days at a time without the harmful effects produced by amphetamines, cocaine, caffeine, and the like. The new world created by learning drugs and brain enhancements is here. I've read about it in sci-fi books, but man, it's gosh darn nifty when science fiction becomes reality. (Kinda makes you feel all warm and fuzzy inside, don't it?)

There already exists a fertile market for mind enhancements. A number of websites offer these drugs for sale. Some sites even go as far as to have real MDs on staff that "legitimize" prescriptions for each sale after filling out a brief questionnaire. If you answer the doctor's questions correctly, you get the drugs, just like in real life. Heck, you can even buy in bulk. Tempting, but I don't feel like getting arrested with kilos of prescription drugs. "Possession with intent to distribute" doesn't sound like something I feel like spending time in jail for.

There are many nootropic drugs on the market. After a little research, you realize just how common they are becoming. The results can be very surprising.

Drug Information and Side Effects

Deprenyl: A selective MAO-B inhibitor created to treat and prevent Parkinson's Disease, it has been found to safely increase alertness which in turns allows one to be more motivated to accomplish tasks.

Modafinil: The precise mechanism through which Modafinil promotes wakefulness is unknown. "Tested and proven to allow one to stay awake and alert for up to 48 hours if taken correctly" (yeah I got a little excited when I read that). There are few side effects and they tend to be mild. So far there has been no indication of possible death due to overdose. Simply taking the person off the dosage will return them to normal. One side effect seemed to be impaired speech; however, upon reading further, I found that this was after having been up for extended periods of time. I can imagine that certain parts of the brain may not respond to this drug, and I know that when I've been up for two days, my speech is a bit slurred too. However, documentation states that motor skills and logic centers remain alert.

One word of caution: though not the manufacturer doesn't like to talk about it, Modafinil has shown to have affect the immune system. I can almost guarantee that this is because the brain is not allowed to enter the sleep-state responsible for repairing this system. I'm fairly certain that the manufacturer is aware of this as they have released a new and improved model called Nuvigil, but that's for another day.

Piracetam: A cyclic derivative of GABA, it is shown to increase cognitive function and communication between the two hemispheres of the brain. It is also thought to increase the number of cholinergic receptors in the brain. This drug has been prescribed in cases of Alzheimer's, ADD and hypoxia, for which it has been seen as a distinctly beneficial treatment. Mild headache and increased appetite can occur, as your brain is using more choline and more glucose due to a higher cerebral metabolic rate.

Neurogenex : A combination of brain enhancement drugs, Neurogenex is designed for longer-term use than drugs like Modafinil. Most of the drugs in this cocktail kick in instantly, but some take about two weeks before showing any signs. Widely used among Ivy League types, this medication has shown remarkable results and few side effects.

As with most drugs, you should not combine these with alcohol or certain medications. And none should be taken while pregnant.

I will focus on Modafinil and Piracetam for this article due to their popularity and distinct characteristics.

While researching these drugs, I was most intrigued by Modafinil because of how well it works. It lets you stay awake. There is no crash after taking it for a period. Overdosing to a dangerous level is difficult. It's out of your system in about 15 hours. There have been similar drugs in the past but they've all been severely controlled. Due to the side effects and toxicity, they required constant vigilance. Modafinil, however, was designed so people could take it on their own, safely and, as an alternative use, an enhancement. Drug companies would love to see this product become available over the counter; however, there is a bit of skepticism due to the somewhat recent ephedrine fiasco, which in my opinion never should have gone as far as it did. Common sense would tell you that the drug was bad for your cardiac system.

When I tried Modafinil, I found myself in a curious state of wakefulness. Curious because it was very mild and felt more like rejuvenation after my tiring day at work. Upon testing by playing a video game, I found my self more effective in game play. I had previously had trouble getting past a certain level in the game. An hour after taking Modafinil, I found myself getting past that point with ease. I felt as if I was retaining and using information better than before. After I hit another point in the game where I kept dying, I decided it was time to go read a book. I am quite proud of my library; however, I find myself rarely able to focus enough to be able to read. This problem didn't even occur to me as I started flipping through my hardbound edition of *Gray's Anatomy*.

I decided to research the further capabilities of this drug and try sleeping only 8 hours every other day. I figured out a dose timing plan and went for it. This proved very successful and I made a lot of progress in my studies and research during about three weeks of this practice. The key, I found, is proper nutrition. I required four meals a day on non-sleep days. But throughout the entire ordeal I was very vigilant and able to carry out my daily duties easily. The only annoyance was a slight headache now and then; this went away when supplemented with Choline. Now, I would never recommend trying this for such a long period, as doing so will most definitely wreak chaos on your system.

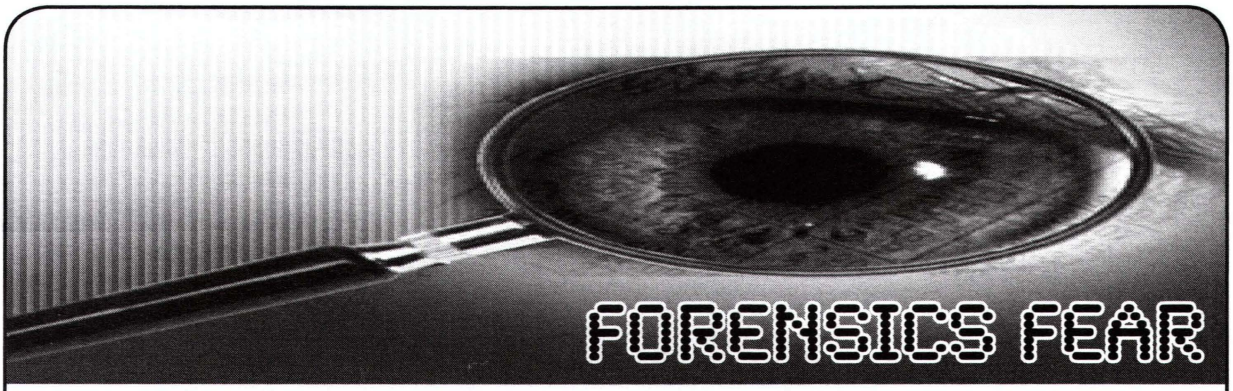
I then found Piracetam (also known as Nootropil), which is fairly easily available for all accounts and purposes and, from what I read, very safe with a mild non-stimulant effect. I found this to be quite accurate. After a brief "loading phase" I found my long and short-term memory improving. Long-lost memories came back and new acquaintances' names were effortless to remember. There was a distinct increase in reflexive motor function and even hearing. I can catch things that others knock over in mid-air, and have no trouble making out lyrics of songs on the radio. My overall attitude has improved as well.

As with Modafinil, I would suggesting supplementing Piracetam with DMAE or Centrophenoxine. My opinion of the two is that Piracetam is much safer and creates the results I'm looking for perfectly.

I did not write this article as a "how-to guide" by any means. It should only serve as a means of informing those otherwise ignorant of the new age we are entering—one where higher IQ comes in pill form, and reflexes like Jet Li's are sold at the pharmacy.

Thank you for reading. I hope I have helped answer some questions, but I hope even more that I have helped you create many new questions of your own. Keep in mind that your brain is a precious thing. Self medication is dangerous, especially with powerful cerebral drugs such as these. You could possibly damage yourself severely. Remember, only a few neurons stand between a properly functioning brain and turning yourself into a cactus.

"Brought to you from the makers of sharp things." Shoutouts to Port7Alliance, GeekLoveRadio, and The DDP. Keep freedom free.



by Anonymous Chi-Town Hacker

A couple of years ago, I started a job working with a forensics software company. Their product is probably the best software on the market by far, but the company just released a new product that has made me question whether I want to stay in this position. This software has the potential to allow Big Brother to search our computers, without us knowing it.

Allow me to explain: In the old days if someone did something wrong, we would go out and black bag the computer, bring it to a lab, and use a forensic tool to extract data for a warrant. This technique is still used today by many companies. However, technology now allows a forensic examiner to avoid the need to go to the physical location. The examiner can use tools to go over the Internet to search for and retrieve all the data for the warrant. This is being done a lot more, as it is much more cost-effective this way.

Now, a forensics examiner has the ability to put a piece of code (POC) on every computer in a given company and to extract data from all suspects in question at one time. If you have 10,000 computers and you are looking to see how someone leaked the Q3 data early, no problem: nine clicks of a button, and you're done.

Almost every Fortune 1000 company is either using or thinking about using this tool. Try to telnet to port 4445 of your workstation and see if you connect to anything. This is the default port, but the company can change it to anything they want. If you connect, then there is nothing on the computer that you can do which I can't tell or show you at a later time. The default process name is `enstart.exe`, but this can be hidden or renamed.

This software is unreal.

How does it work?

Essentially, the POC runs as a root kit on every workstation and server. The forensic tool connects to the POC with a GUI, secured with PKI PGP authentication. The forensic POC runs underneath the operating system, so you can look into anything the OS is doing. Also, because it is not OS-dependent, hidden directories, embedded code, changed files or even other rootkits will be detected instantly. It also has the ability to see volatile memory, which means that processes, current users, and network ports can all be seen in real time. If you are running a trojan in memory, then it will be found. If you are using netcat or bifrost, it will be found.

What else can it do?

Because the POC is underneath the OS, it has the ability to act on all 10,000 computers at once. It can wipe sectors, kill processes, and close ports.

There is also a plugin for IDS systems to make it easier to weed out false positives. If a server is being hit with an attack, the IDS can tell the tool to go to the computer in question and to collect evidence on whatever is happening.

It can look at a computer, compare it to a previous search, and see if anything has changed.

What's the big deal?

Imagine what could happen if the government put this POC on every new computer to come out in 2008. *Every* government agency is already using this software. Another issue would be if someone figures out how to use the POC on these computers. Hello, unlimited power! Imagine having full access to every server, workstation, and laptop in a Fortune 50 company.

Although this company has been very good to me, I feel it is not right that such knowledge– and knowledge is power– is given to watch over us. You are now aware of the tools being used to see you.

How do I stop the tool or make it harder for the tool to see what I am doing?

Simple security measures can be taken, for example:

- Full disk encryption is a great start, but your company policy may prohibit this.
- Look into the U3 encrypted drive.
- Consider VMware with encryption, putting / boot on USB.
- Investigate bootable CD's with encrypted USB.
- Learn new anti-forensics techniques and tools, such as Sam Spade and touch.

I hope this will help educate you.

Tesla's Wireless "World System"
To Turn Earth into One Gigantic Dynamo

Transmissions

by Dragorn

What does a guy have to do to not get noticed around here?

You are no longer a shadowy figure on the Internet. A dynamic IP will not increase your mystique. Your nested anonymity routing system will not hide who you really are. The Internet Santa Claus knows if you've been Googling for naughty or nice, and he knows you haven't been sleeping at 3 am. Internet Santa is coming to your town to make sure you've seen every possible advertisement for the latest TV show, gadget, or method for enlarging your nether regions for the holiday season, and Santa needs to get paid.

There are hundreds or thousands of bits of information about where you are, what you buy, and what ads you've watched (and what ones you've skipped), what books you read, what search terms you look for, and what sort of email you get. Each piece of information is of limited value until someone links them together - suddenly the disparate fragments of your behavior become a single record set revealing more about your habits and interests than you might think (or want).

The first ghost, that of privacy past, takes us back to 2006 when AOL released a large database of anonymized search data for public research: within days, several groups had associated the search terms of the users to build profiles of users, even multiple users of the same system, and in some cases it was enough to track down individuals to real-world names and addresses. Despite quickly realizing their error and removing the search data, it had obviously spread too far to contain and is still available. Let's look at this again: After removing all user-identifiable information from the logs and hashing users down to a single number, it was still possible track down someone in the real world.

The second ghost, that of privacy present, shows us what can happen when companies share data. Monitoring the browsing habits of millions of users is trivial when those users volunteer their information, likes, dislikes, and friends. Social networks have often been considered a major privacy risk, but the risks are directly tied to the information that the user is willing to share. In November 2007, Facebook partnered with several companies to share behavior and purchasing data from other sites. The "Beacon" feature links a user's Facebook identity with their behavior on other sites by allowing access to the Facebook information.

Multiple commercial sites, such as Overstock, Fandango, and The New York Times review sites link to the Beacon system and aggregate purchase information with a user profile. The most public outcry is due to this information being displayed to other users viewing the Facebook entry, but no matter how (or not) the information is displayed, the behavior has been recorded and correlated.

The biggest privacy invader of modern systems is the web browser. Browsers are large, complex pieces of code which handle untrusted (and frequently hostile) data from anonymous network sources. Excluding vulnerabilities and exploits to the browser code itself, modern sites are attempting to turn a stateless unauthenticated system into a stateful, strongly authenticated system to refer to dynamic data. Browsing leaves a continual detritus of cookies and session data linking who you were with where you are now. The browser is a constant across changing IP addresses: Who you were the last time is who you are now, regardless of how you

got there.

Our greatest convenience is our greatest downfall, as is often the case with security. "Remember me" is the most innocuous and obvious of the risks - ad services each place a tracking cookie which can monitor your movement across multiple websites. The most obvious, but by no means the only one, is Google Analytics. Google achieved deep penetration by including useful, free, and (to the average user) non-obtrusive tools. Website maintainers include a bit of javascript, and get a wealth of useful information about visitors. Estimates of coverage are hard to find, but it is pervasive. The downside? Every site which contains an Analytics entry updates the bread crumb trail, building a model of who you are and where you go. Privacy networks such as Tor can protect traffic and origin, but can't prevent an application on your system happily updating the bread crumb trail.

Sure, the majority of these services are anonymized so that no directly identifiable information is returned. However, a look to the past shows that obfuscated information may not be enough to prevent identifying information from leaking, and the services you use may be actively working against your privacy interests: Providing advertising data is a lucrative business model.

Finally we come to the specter of privacy future, traditionally the most frightening of the trio and in this story no less so. "So what," you may ask, "I don't care if they want to send me ads, I block popups, and what's wrong with getting ads for products I might actually care about?" Absolutely nothing. But once that data modeling your behavior, inclinations, and opinions exists, it is there forever, simply a subpoena away from the next witch hunt for whatever are considered the latest unpatriotic activities.

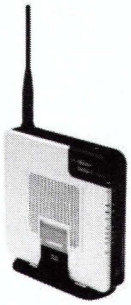
In 2006, the U.S. government launched a subpoena process for search data from the major search providers: Google, Yahoo, AOL, and Microsoft. Of the four, only Google fought the request. While the request was only for search terms, with absolutely no user-identifying information (even the one-way hash AOL used to link queries by the same user in the previously released data), it shows that the courts are aware of the availability of this information.

In June 2007, federal prosecutors attempted to force Amazon to disclose customers who had purchased books from a specific seller. The case centered around tax evasion on the part of the seller, however it served as an additional harbinger of attempts to use online tracking data well beyond the presentation of advertisements, and the judge who ruled in favor of Amazon in November agreed, calling it "troubling because it permits the government to peek into the reading habits of specific individuals without their prior knowledge or permission."

How do we prevent this future from happening to us? Unfortunately it's not going to be as easy as buying the biggest turkey in the store window (and that's where I'll end the holiday metaphors). Browsers have begun to add privacy-enhancing features: Firefox can automatically clear the cookies, cache, and browsing history on exit, for example. However, these measures won't help against tracking within a single browser session, and a significant model of behavior can still be built. Disabling all tracking functionality in the browser by turning off cookies, javascript, java, and flash will prevent tracking by anything but IP address and HTTP referrers, but will render many sites unusable. Some mitigation can also be found by using tools such as Greasemonkey or Adblock to filter the URLs which provide the tracking information: www.google-analytics.com and ssl.google-analytics.com are easily blocked, but affect only tracking by Analytics and not other sites.

There is likely no silver bullet besides vigilance: Be vocal, hold the services which hold your personal information to the commitments in their privacy agreements, and avoid dealing with those who don't or who have poor privacy policies. Opt out of information sharing whenever possible, and complain when it isn't made possible.

Happy browsing to all, and to all a good night.



CRACKED SECURITY AT THE CLARION HOTEL

by Gauss VanSant

I recently stayed at the Clarion Hotel in Albany, which offers free high-speed Internet to its guests. During my stay, I decided to poke around on hotel's network. I had heard horror stories about hotel networks and wanted to see if they were accurate.

The hotel contained three different wireless networks that I could identify. The first network used the SSID "ClarionInn". It was unsecured and broadcasting its SSID. I connected to the network and was immediately disappointed with the network speed; if this was the hotel's "high-speed Internet," then the advertisers deserved to be drawn and quartered.

I ran the standard Linksys router security test: browse to 192.168.1.1 and enter the default passwords for the router. If can't be bothered to look the default up, don't have it memorized, and happen to be lousy at guessing, try username: admin, password: admin. The connection failed without displaying a password prompt, so I assumed that the router had been set up to disable wireless administrative access, but just to be sure I checked my computer's IP configuration. Surprise surprise, 192.168.1.1 was not my default gateway, and as it turned out, whatever I had connected to was not even using a private IP address. In retrospect, the device was probably a wireless modem/router combination, but after a nine-hour drive, this didn't occur to me, so I simply retried the "Linksys for Dummies" test, watched it fail, and passed out.

The next morning, I wandered over to the hotel's public computer lab. This consisted of two computers, one running Windows XP, the other running Windows Vista. I sat down at the XP box, which was already logged in, and did a bit of idle web browsing. Only a bit, though; I quickly discovered that HTTPS was being blocked, although straight HTTP worked fine. At first, I thought that this might be an overly paranoid firewall configuration, but the neighboring Vista box worked perfectly well.

I looked around the installed programs list, thinking I might find some sort of childproofing filter installed, but instead I found good reasons for the hotel to lock down network ports. One thing Vista has right, and the thing which probably saved that box, is that it requires a password to install any significant software. On the XP machine, I found World of Warcraft, Second Life, and, my oh my, Family Key Logger. Well, that can't be good, can it?

I started up the keystroke logger and saw it pull up an icon in the Quick Launch bar, which included an option to view the keystroke log. Well, what would you do? In addition to some test text I entered to see if the program was working, I discovered some lengthy chat transcripts from a program listed as Mail.ru, which turned out to be a Russian language chat client. I also found a username and password for a Citibank Australia account, and some e-mail transcripts from the same user. Oh, hell.

Putting aside that moral dilemma (vacation in Honolulu, anyone?), I looked around to see why the hotel computers seemed to get such a fast network speed while mine was so lousy. As it turned out, the hotel's second wireless network was not broadcasting its SSID, "QUALITY", though it otherwise appeared to be just as unsecured as the ClarionInn network. I headed back to my room to log in.

High-speed Internet, right? No. I couldn't connect to QUALITY and couldn't figure out why, so I decided that the hotel had set up MAC filtering on the router. This may not seem logical at first glance; after all, the hotel clearly hadn't bothered with any other security. But it did make some sense when I discovered a note that hotel customers could come to the front desk to pick up a wireless card for the hotel network.

Here's how not to hand out a $60 piece of computer equipment: Do not ask for identification. Do not ask the person what room he or she is staying in. Do not ask the person to sign his or her name. Do not write down any identifying information about the device. In fact, do not do anything that would prevent anyone from walking out of the lobby and pawning off half of your network infrastructure.

So I picked up a card and tried it out. Now I could connect to the QUALITY network, but my signal strength was miserable: 1% at best, and none at all if I moved in the wrong direction. Since the ClarionInn network had a much stronger signal, I guessed that the card was a dud and spoofed its MAC address on my own wireless device. Still no joy. Eventually, I tried connecting from the hotel's computer room, which, it turned out, worked even without the MAC spoofing.

Go figure: I'd given the hotel credit for implementing a basic security measure when, in fact, they simply didn't have proper signal coverage for their high-speed network. I would understand if it were intended to be used by the hotel systems only, but the desk person who gave me (er, let me borrow) the wireless card specifically told me to connect to the QUALITY network. So, if guests were supposed to be using it, why wasn't it broadcasting an SSID?

I believe I mentioned finding three wireless networks earlier. The third was a near-exact copy of the ClarionInn network, ClarionInn1 or something like that. Its signal was so weak that I never bothered to play with it; presumably, it

was covering the other end of the hotel. At this point, I decided that the hotel networks weren't worth poking at, short of locating the hardware and plugging in an Ethernet cable, and I wasn't about to do that without a spotter.

I headed back to the hotel computers and checked in on the XP machine. By this point, someone had logged out of the guest account, killing the keystroke logger, which raises the question of what point there is in a keystroke logger that a five-year-old who understands the concept of right-click could disable. But I digress. I logged back into the account and got this pleasant message for my troubles:

"Dear Hotel,

Your security is awful. You're just lucky I was too lazy to break into your admin account."

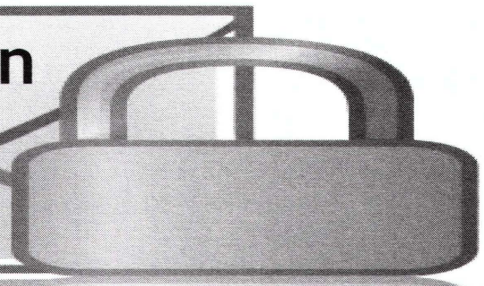
I'm paraphrasing, but honestly it wasn't much more intelligent than that, popping up in a DOS window on login. The amusing part was that when I sat down at the computer, the administrator account had been left logged in, and pretty much anyone with a finger could have simply clicked their way into it. Presumably the "l33t hax0r" had actually broken into the box over the network. Yet another reason to avoid the box like the plague, but the box was turning into an onion for me: tasty and lots of layers, but peeling them back made me want to cry.

Viewing hidden files and folders turned up a Remote Desktop program in the Documents folder; if this wasn't a back door that the script kiddie had set up, then it probably was the thing which let him in to the system. I also turned up another key logging program, Perfect Keylogger. This one was a bit stealthier than the other one, in that it didn't pop in the All Programs menu wagging its tail and smiling. I suppose I could have looked for some logs for this program as well, but at that point the box's virus scanner pinged me about a new piece of malware that was busy installing itself, and I felt a strong urge for an antiseptic and some sleep.

The next morning was checkout time, and it was only with a great effort of will that I didn't grab passing staff by the collar and start screaming about least privilege. Returning the wireless card involved no more checking than acquiring the thing had; in fact, I still have a driver disc for it that I really ought to think about mailing back.

The moral of the story? Don't touch a hotel computer. If you must touch a hotel computer, and you have the option, pick Vista over XP, because a blind stab at security is better than nothing. And, no matter how important you think it is, do not log into anything of value. SSL is no defense against a keystroke logger, and for all I know that poor Australian's bank account is still out in the open.

Building Your Own Safe, Secure SMTP Proxy



by sail0r
sail0r@creepjoint.net

Shows of power are very common in the business world when a new executive takes power. The reasoning, I have been told, is to make a powerful first impression that you are the big, bad new boss.

Recently, the CEO of the small software company I work for was replaced. After several weeks, the new CEO began to wield the ax. At first, a few fringe benefits such as catered meetings and periodic team gatherings at the local pub were gone. Next came the restrictions on internet use. Internet traffic is now logged and filtered. AOL IM traffic is now routed through a proxy and logged. And, closest to my heart, SMTP restrictions are now in place; all outgoing mail must now be sent through the company's SMTP server where, of course, it is logged. Until this point, I had been happily accessing and sending my personal e-mail with Thunderbird and my personal IMAP and SMTP servers. Webmail services such as Gmail are out of the question as alternatives, as these sites are now blocked and HTTP requests for these sites are now logged.

Furthermore, since all network traffic is now being logged, any attempt to circumvent these restrictions must be disguised as valid network traffic. Since ssh and scp must remain open for valid business use, I have devised a method whereby I may continue to use Thunderbird to send my personal email from work but use ssh and scp to proxy the outgoing messages through a personal shell account. This has the excellent added benefit of encrypting my outgoing mail, hiding it from corporate snoops.

The method I use consists of four parts:

1. A custom SMTP server runs on my local machine on some arbitrary port. To make detection slightly more difficult, I do not use the default SMTP port of 25. As of this writing, there are no in-house port scans. Management does actually realize that developers writing network code often have works-in-progress running on multiple high numbered ports.
2. The custom SMTP server will accept messages like a normal SMTP server. The message is then copied with scp to a directory on a machine on which I have remote shell access.
3. A cron job runs every minute to poll

the message directory and send the messages to their destinations.

4. After each message is sent, it is moved to an archive directory.

After I had a rough outline of my approach in my head, I decided to actually implement the idea using the Python programming language. I made this choice because I have found that Python's compact and powerful language constructs often make coding go faster than it would with other languages. Also, there are many ready-built APIs available. I was certain that I could easily find code which would handle the ssh and scp as well as the eventual SMTP connection. The only code I would have to write would be to glue together ready made pieces. In this regard, Python certainly met my expectations. The code which I wrote is a good example of code re-use and the power of Python.

To begin, the install following non-standard python modules: pyDNS (`http://pydns.sourceforge.net/`), smtps.py (`http://www.hare.demon.co.uk/smtps.py`), and pexpect (`http://pexpect.sourceforge.net/`). Obviously, you will need a shell account on a machine someplace that has an ssh daemon running. Also, it is assumed that you have the ssh and scp command line tools installed on your local system and in your path. One security note: for the ssh and scp commands, you will either need to put your password in the script or use ssh keys. In the included code, I embed my password in the script. If you do this, you **must** chmod your script to be 0700, so no other users of your system can read your password. I believe that this is just as good security as the use of ssh keys. If someone got root on your system, then they would be able to use your ssh key to login to your remote server just as easily as using your password. Use whichever you are most comfortable with.

After you have installed the prerequisite modules, the SMTP proxy consists of two programs. `SMTPLocalService.py` is to be run locally. I run this on the same machine I am running Thunderbird on. `SMTPLocalService.py` runs via cron on the remote host.

For the sake of simplicity, I just start the script SMTPLocalService.py from the command line as follows:

```
python SMTPLocalService.py 1234
```

In this example, I set the port to be 1234. Of course, you may choose any port you wish.

`SMTPRemoteService.py` is set up via crontab. Here is how it looks in my cron file

```
* * * * * /usr/local/bin/python /home/sail0r/smtp_out/SMTPRemoteService.py
```

Note that this just runs every minute of every hour of every day. Again, how often this runs is up to your discretion.

Finally, you must tell Thunderbird about your new SMTP server. Go to the Tools menu and select "Account Settings...". From the menu on the left hand side of the window, choose "Outgoing Server (SMTP)". Select the "Add..." button. Now, simply enter the name of the machine running `SMTPLocalService.py` and the port that you have chosen. Set this as your default SMTP server, and now you will be able to send outgoing safe, secure outgoing mail, free from prying eyes!

Please be aware that I make no claim that this is bulletproof code. Astute readers will notice that mail is now being sent asynchronously. Failures in `SMTPLocalService.py` usually, but not always, cause an error to be propagated back to Thunderbird. Failures in sending the mail from your shell host will need to be debugged from the server by manually running `SMTPRemoteService.py`.

In this article, I exclusively use Thunderbird as an example, but this should work just as easily with any email client assuming you configure the SMTP settings correctly. These scripts were developed on Unix; however, they will easily work with only slight modification with Python on Windows.

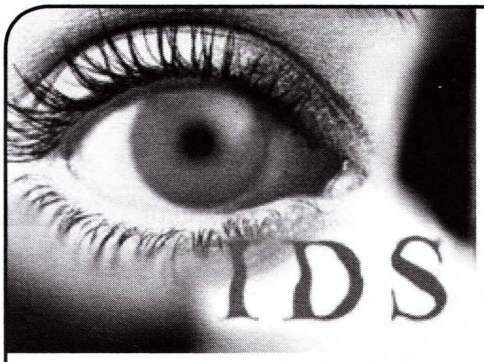
Anyone with further questions or comments may contact me in #2600 on the 2600 IRC network, via ICQ 490590026, or at sail0r@creepjoint.net.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.



Zero-Knowledge Intrusion

by S. Pidgorny

This article is about evasion of intrusion detection systems: whoever monitors activities on the target network should have zero knowledge about these activities. Before continuing, I must warn that unauthorized access to information systems is crime in most countries. The point of this writeup is awareness of the possibilities, which will help protecting infrastructure.

Zero-knowledge intrusion is based on two principles: perform only passive reconnaissance, and do not ever generate traffic that is not generated by legitimate clients on the network. Intrusion detection systems are based on anomaly detection. You just don't create anomalies.

```
LAN ---- Hub ---- Victim
                  |_____ Agent
```

Why this is better that just locating an available port or disconnecting the victim system? Because it doesn't create anomalies: there are no new connections to the port on the LAN switch, and only temporary disconnections of existing systems. As such, alarms probably won't be raised. Of course, you need to power the intrusion agent using some kind of power source, and hide it—but modern office buildings seem to be designed for just that. Audits of power-consuming devices are unheard of. Entering the building is beyond the scope of this article; I refer you to Hollywood movies for ideas.

A very important aspect is remote control of the intrusion agent. My preferred way is to use mobile data services available on commercial GSM and CDMA networks. This is better than Wi-Fi because companies sometimes employ specialized "wireless" intrusion detection systems which focus on detecting the presence of alien Wi-Fi devices on premises. There is also the ability to control the agent from pretty much anywhere in the world. A dial-in IP connection to the agent is one option. A better approach is to connect the agent to an intermediary server and go through that.

Start the reconnaissance without using an IP address. Make sure you don't assign an IP address and don't start a DHCP client on your Ethernet interface; use "`ifconfig eth0 up`" to activate the interface. This is sufficient for running tcpdump or another traffic sniffer. You have to capture traffic for a few days and analyze the results. The information you're looking at includes, but isn't limited to, DHCP and DNS configuration, Windows infrastructure (such as names, domain controllers' locations), messaging infrastructure details, software distribution and active network monitoring tools. All traffic of the victim system will be available for sniffing, which helps greatly: on a stand-alone port, only broadcast-type information would be available.

The second stage of zero-knowledge intrusion involves IP connectivity and generating network traffic. The way we connect to the victim network also helps here: it allows connecting to the IP network even if 802.1x port security or another endpoint security mechanism is used. The intrusion agent will have to have the same MAC address for the LAN connection as the victim host and have netfilter configured to deny all inbound connections. See [1] for further details.

Cloning is a powerful technique and an important part of zero-knowledge intrusions. There's an interesting application for it which allows connecting to secured wireless networks. Let's say the target organization deployed a WLAN according to Microsoft's secure WLAN deployment guidelines, using either PEAP and passwords or EAP-TLS and certificates for authentication (see [2a] and [2b]). Elements of the solutions include dual computer/user authentication, a RADIUS server with a TLS certificate, and strong traffic encryption with dynamic random keys. These components are all very secure—unless you can clone an authorized client system. Only opportunistic intruders steal documents and artifacts; those with a plan and determination make copies. Since the system that has been cloned is not stolen, alarms are not raised. Take a Windows laptop system image, install it on another laptop, change the local administrator password, change the AuthMode registry value (under HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\) to 2, and reboot. Now the computer will authenticate with its own credentials, either password or certificate, and you are connected to the secure WLAN. That is another way of connecting the intrusion agent without physical intrusion or presence.

Now, when you have IP connectivity, the rule is *not* to use any type of network connection that is not used by legitimate clients, as seen in the information collected during the first stage of intrusion. This is very important. There are many "ethical hacking" courses, and they pretty much all suggest using tools like nmap (see [3]) for network mapping. Don't—not even with the

paranoid timing option. The rationale is simple: if you run "nmap -T Paranoid host.internal.example.com" then some unusual connections will be attempted. Unusual is suspicious. Intrusion detection systems may be configured with a rule that echo service (on ports 7/tcp and 7/udp) is not to be used anywhere on the network. The nmap run will trigger the alarm with a single packet. However, NetBIOS over TCP/IP is considered normal on most networks, so you can sweep subnets using tools like NBTScan (see [4]) without triggering alarms, because connections on 137/udp are "good."

In the end, you have a system that is connected to the network and knowledge about the normal behavior of network clients. This provides an ideal base for an active attack. The zero-knowledge status will end at some stage. But by limiting the attack to the use of information obtained using social engineering elsewhere, the window of opportunity for attack can be greatly extended with specific weaknesses of the network in question and zero-day exploits against protocols that exist on the infrastructure. *Shouts out to the Coffee Company of Balaclava, hello to ES, and good luck to the P&A squad.*

Web References

[1] Getting Around 802.1x Port-based Network Access Control Through Physical Insecurity (http://➥sl.mvps.org/docs/802dot1x.htm)

[2a] Securing Wireless LANs with PEAP and Passwords (http://www.microsoft.com/technet/➥security/guidance/cryptographyetc/➥peap_1.mspx)

[2b] Securing Wireless LANs with Certificate Services (http://www.microsoft.com/technet/➥security/prodtech/windowsserver2003/➥pkiwire/swlan.mspx)

[3] Nmap - Free Security Scanner For Network Exploration & Security Audits (http://insecure.➥org/nmap)

[4] NBTScan. NetBIOS Name Network Scanner (http://www.inetcat.net/software/➥nbtscan.html)

Booting Many Compressed Environments on a Laptop

by Scotty Fitzgerald

Disclaimers: All standard disclaimers apply, especially ones about reading manuals before trying, backing up data and using a box without important info on it before trying anything in this article. Mileage may vary.

This article is about how to use a few Linux/Unix command lines to be able to carry several operating systems in a compressed form on a laptop with limited disk space. Before getting into the "meat" of the article, I will explain what inspired me to figure out this way of doing things, so the reader can see when it might be useful. After learning the techniques presented here, the laptop user will be able to do the following:

- Carry a laptop set up for dual booting, but have more than two complete OSes actually stored on the laptop.
- Be able to uncompress and activate a compressed image of an OS instance in about ten minutes
- Be able to compress and deactivate an uncompressed OS instance in about ten minutes, or, alternately, to revert any changes made during a usage session, simply by choosing not to compress the session.

Here is why I figured out this technique: I recently had a trip to visit a relative in another state. At the same time that I was preparing for this trip, which included my planning to take my laptop for offline computing needs as my relative does not have net access, I realized that Verizon might need me to have a Windows partition set up for a distant but upcoming fiber conversion. I really am not fond of Windows and don't use it, but apparently Verizon has something against non-proprietary OSes. I really resent it, as I would rather use that disk space for something useful, such as backups or mirrors, instead of wasting it with an OS I don't use. This led me to begin toying with the idea of compressing it somehow while not in use. I also teach at a local computer club, and wanted to boot into other distributions of Linux and FreeBSD so I could test things on multiple distributions to see if they work before giving my lectures. All this forced me to learn a way of compressing and "swapping out" a whole operating system to "swap in" and use another.

The technique works, and I have personally field tested it. It only requires six standard Linux/Unix commands: dd, cfdisk, gzip df, rm, and nano or pico. Theoretically, parts of this technique can be used just for backing up whole systems, or a Linux "Live CD" such as Knoppix could be used to run the commands, and thus a Windows user could switch between different versions of Windows

for whatever reason.

For the sake of brevity, I will make a few assumptions. One is that the reader is tech savvy enough to have set up the GRUB boot loader in the MBR and the "alternate" OS (whatever that might be) in the partition `/dev/hda1`. I will call this partition the "swing partition," as different OSes will swing into uncompressed activity in this disk space. Most users will come to this article with a Windows installation in the swing partition, and a Linux one in the first extended partition, which is usually `/dev/hda5`. Again, after understanding this technique, it is easily modifiable to suit different customized situations.

Let's start with a look at the GRUB bootloader in a typical dual boot situation. On a typical installation, GRUB resides in the computer's MBR and uses a file called `/boot/grub/menu.lst`, which resides in the Linux partition. The `menu.lst` file is a simple text file which presents the boot menu to the user. This menu looks like a couple of boot options for the Linux system, then a separator that says "other operating systems" and a few automatically-generated lines for your Windows installation. From a Linux command line prompt, open up the `/boot/grub/menu.lst` file with your favorite text editor. You will notice that the Windows entry has the command "`chainloader +1`" at the bottom. This is the first key to understanding how to complete our project. This command tells GRUB to go into that partition and load whatever boot loader is in that partition, which in this case is Windows'. Therefore, whatever you have in that first partition will load and run as long as it has a boot loader in the partition with it, rather than having its boot loader in the MBR. This is why on my system I changed the menu from "Windows whatever" to "Chainload Partition #1."

So after making any desired changes to GRUB's menu, the first step is to copy the whole partition to a compressed file. The beautiful thing about the command line is its power: with a pipe and two commands we can copy that whole partition, byte for byte, including its format (FAT or NTFS) to a data file on Linux. This needs to be done as root, because only root can access a whole unmounted partition as a device under Linux or Unix. I first set up a directory called `/backup/images` to hold my images of the swing partition. Here is the command to make the image:

```
dd if=/dev/hda1 | gzip > /backup/
➥ images/windows.hda1.gz
```

Let me explain. The first part of the command is "`dd`", which is the disk-to-disk copy command. When given the parameter "`if=/dev/hda1`", it makes a byte for byte copy of the partition, including the format, garbage, data, and everything else, and sends that to standard output. (If you had used a second parameter, "`of=somefile`", you would get an uncompressed image of the disk.) You need to pipe this to a compression program in order to save disk space, so pipe it right into `gzip`. `gzip` makes a zip file from standard input to standard output, so direct the output (the "`>`" directs output) to a file. Later on, I'll touch on how to optimize the compression before running this command, but let's jump right into how to restore a partition.

As you have probably guessed, the command to restore the partition is pretty much the opposite of the imaging command. The command is

```
gzip -cd /backup/images/windows.
➥ hda1.gz | dd of=/dev/hda1
```

Here, the gzip command is called with the options "-cd" which tells gzip to decompress and throw the result onto standard output. That standard output is piped to the dd command with the output file set to the partition to which we want to write.

As we stand now, we have a nifty way of backing up a whole partition using only a few standard commands. But let's see how we can extend this to put an alternate system into the swing partition.

First, swap out whatever is in the swing partition. Then, use a disk partition editing utility to delete the partition `/dev/hda1`. I like to use cfdisk, which is a text mode graphical partition editor, but anything that can delete the partition will do the job. The important thing is not to change the size of any of the partitions, because that will cause the image files you create with dd to be either too big or too little. So delete the partition without modifying the other partitions.

This will clear the way for you to install another system into the swing partition. All you need to do is to put your installation CD into the CD drive and reboot. The installer of the new OS will then see an empty slot in the partition table. After installing and setting up the new OS, you use the same commands to copy off and compress the swing partition, and then use the restore command to bring in whichever system you want into the swing partition. Just make sure that when the installer of the new system asks where you want to put the boot loader, you don't overwrite the MBR! For this to work, that MBR needs to remain untouched, so place the boot loader into the partition with the system.

The astute reader will see that this whole things raises an important question, which is that the partition label will be inconsistent. For example, let's say that the last install you did

was FreeBSD. Now the partition table entry is marked as a FreeBSD partition, but when you load a Windows partition into the swing partition, you'll have a Windows format partition with a FreeBSD type label in the partition table. Well, the beauty of GRUB is that it ignores the partition label, so as long as the kernel it boots under can read that partition it will boot it. In my field testing, the only oddness I had was that Windows XP would check its file system because of what it termed an "inconsistent flag." But the check would come back as OK and the machine would reboot into WinXP.

Now, a word on the compression. Remember where I said that image that dd produces contains even the garbage on the disk? Well, that garbage, be it old chunks of now-deleted files or other whatnot, can cause a hiccup. The easiest and most efficient thing to compress, is a long string of the same character, so it would be helpful to write out the free spaces on the disk with something and then delete it. How? We once again turn to the dd command. This command goes like this:

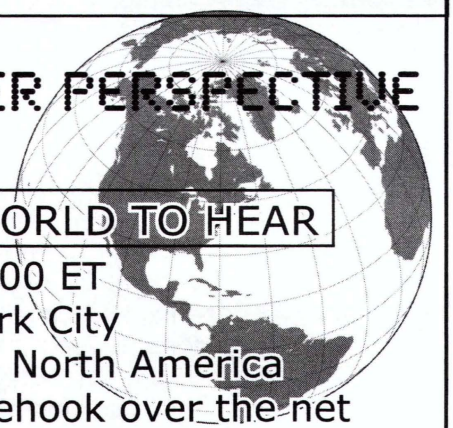
```
dd if=/dev/zero of=/mnt/hda1/
➥ zeros.dat bs=1000000 count=10
```

This command produces a file of 10 megabytes of zeros. Note that, for this command, you must mount the swing partition because you want to create a file within the partition, not to work on the whole partition. Here I mount the partition to `/mnt/hda1`. Then, the input file is "`/dev/zero`", which is a pseudo-device in Linux which just gives unlimited zeros when accessed. The bs is one megabyte, and dd is asked to do this for ten such blocks, giving a 10 megabyte file of zeros. You need to see the free space on the swing partition and adjust this command accordingly (try "df -h" after mounting). Then, run the command, follow it up with a "rm /mnt/hda1/zeroes.dat" to remove the file. This is an easy way of zeroing out unused areas of the disk. After doing this, I managed to get 9 GB partitions with Windows XP, Windows 2000, and FreeBSD compressed down to 1.4 GB files!

As we've seen, standard Linux/Unix commands totally rock with their power! Now you can travel with several different OSes crunched down into small files while traveling with limited disk space. But the benefits of learning these commands does not end there; you can also back up a whole partition before applying an update or installing a program. Then, if you don't like what that update or installation did, you can roll back to your previous state. By keeping several of these previous states copied up to a larger drive such as a USB disk or another computer, you can go back to whatever state you want. Also, if you set up computers for others, you can set up everything in a fixed-sized partition of, for example, 10 GB. Now, you could actually roll out and install really quickly if the hardware is similar enough by just copying out a standardized 10 GB partition. We've also seen how to quickly zero out unused space in a partition, which can have security applications.

OFF THE HOOK

TECHNOLOGY FROM A HACKER PERSPECTIVE



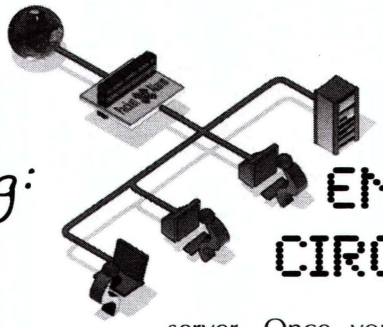
BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite.
Contact us if you can help spread "Off The Hook" to more listeners!

Avoid Web Filtering with SSH Tunneling: ENCRYPTED CIRCUMVENTION



by Tessian
tessian@gmail.com

As an experienced Websense administrator, I was excited to read Major Lump's article about circumventing filtering, "Avoiding Internet Filtering," in the Spring 2007 issue of *2600*. Unfortunately, I was dismayed to find out that that the method he proposed was not an actual workaround but rather a product of a poorly configured Websense integration. The Websense installation in question did not have a service responsible for filtering traffic on non-HTTP ports, so the writer was easily able to circumvent it by visiting an HTTPS internet proxy. Websense and other top-tier internet filtering products rely on integration with another service, most commonly a firewall or proxy servers, to forward normal HTTP traffic. The filters rely on packet sniffing to pick up the slack and to be able to filter not only HTTPS and FTP, but also instant message traffic, proxies, streaming media, peer-to-peer software, and more. Most internet filtering databases contain the IP addresses of well-known proxy websites, so they can block them on HTTPS as well as HTTP. With this in mind and in an effort to stay one step ahead of my users, I decided to start searching for a real method of circumventing internet filtering.

The Solution

My search ended in success with a wonderful method many of you may be familiar with: SSH tunneling. You can find methods on accomplishing this all over the web, but it was the guide at `http://www.buzzsurf.com/surfatwork/` that broke it down the best for me. Basically, we'll disguise your SSH tunnel as an HTTPS connection and forward all internet traffic through it, effectively bypassing all Internet filtering, and firewalls in between.

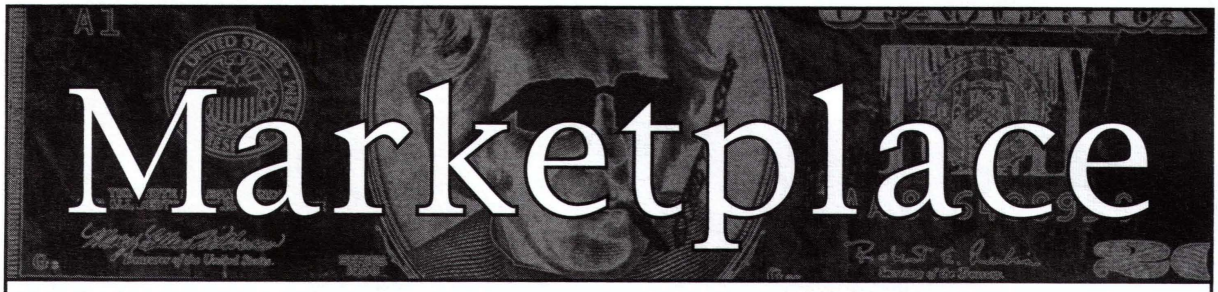
To accomplish this, configure a PC at home as a normal SSH server, but set it to listen on port 443, which is normally reserved for HTTPS. Now, assuming you've made sure this SSH server is accessible from the Internet, you connect to your SSH server. I recommend using a free DNS service such as DynDNS (`www.dyndns.com`) to make it easier to connect back to your PC at home. This is most easily done by downloading or bringing in a copy of putty and at the command prompt running the command "`putty -D 8080 -P 443 -ssh sshserver`", replacing *sshserver* with the IP or address of your SSH server. Once you've successfully connected to and logged into your SSH server, you need only change your browser's settings to use the SSH tunnel you've created as a SOCKS proxy. This is done in the IE's Advanced Proxy Settings configuration by setting the SOCKS address to 127.0.0.1 and the port to 8080. Now your internet traffic is encrypted and virtually undetectable. This can also be used for any other web application that supports SOCKS proxies; simply configure them the same way.

Risks

Obviously, there are risks involved with testing this at work. If your Information Security department is anything like mine, then there are alarms and triggers set around the network just waiting to squeal on you the second that they detect proxy usage. However, assuming you configure this correctly the first time, there will be almost no indication of this because of the encryption involved. Websense logs it as HTTPS traffic to an "Uncategorized IP address." There are only two ways that Websense could stop you: if HTTPS is blocked or if uncategorized websites are blocked. Neither is very likely unless you're in a very small environment, as both have very legitimate uses. The only flag that was raised was by my Intrusion Detection System. I was pleasantly surprised to find out it did in fact notice I was using SSH on a port other than the default of 22 and that it threw an event marked Suspicious. Luckily the event only fires a few times during the initial connection and isn't detected after that. In larger environments, it's not uncommon to see SSH running on an unusual port, but if you have a very vigilant security department, this could be noticed.

Uses

There are more uses to this version of SSH tunneling than just circumventing filtering; this also works very well to protect yourself and your information on untrusted networks such as wireless hot spots. While businesses and universities normally warn and notify their users if they are being monitored, there is no way of telling just what is lurking on an untrusted network waiting to sniff your traffic. SSH tunneling can be used for things other than internet forwarding. With a few changes, you can use it to protect connections back to your home network for email or printing. If you know the port a service communicates on, you can put it through this SSH tunnel.



Marketplace

Happenings

THE LAST HOPE. The seventh Hackers On Planet Earth conference will be held at New York City's HOtel PEnnsylvania July 18-20, 2008. Visit www.hope.net for the latest news. Speakers, vendors, creative participation welcome. Call (212) PEnnsylvania 6-5000 for the special conference room rate. Discuss your plans and suggest ideas at talk.hope.net. History awaits.

CELEBRATE COMPUTER HISTORY AT THE VINTAGE COMPUTER FESTIVAL. The mission of the Vintage Computer Festival is to promote the preservation of "obsolete" computers by offering people a chance to experience the technologies, people, and stories that embody the remarkable tale of the computer revolution. The VCF features a speaker series, a hands-on exhibition of live, working vintage computers from all eras of computer history, a marketplace, a film festival, and more! This year we celebrate 10 years of the VCF, so this event will be the biggest and best ever. For more information, visit http://www.vintage.org. The game is afoot! www.vintage.org/special/2007/vcfx/

For Sale

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Now available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! *2600* readers get 10% discount on TV-B-Gone keychains - use Coupon Code: 2600. www.TVBGone.com

JEAH.NET supports *2600* because we read too! JEAH.NET continues to be #1 for fast, stable FreeBSD shell accounts with hundreds of vhost domains, FreeBSD and Plesk web hosting, 100% private and secure domain registration, and aggressive merchant solutions! *2600* readers' setup fees are always waived at JEAH.NET.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v24no4" and get 10% off of your order.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high quality glossy color poster is available in two sizes (16"x20" and 20"x30") and makes a spectacular gift for engineers, scientists, radio & television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new Access All Areas, a guidebook to the art of urban exploration, from the author of Infiltration zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that's it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by simply dangling your whistle and saying nothing. Cover one hole and get exactly *2600* hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item, but also a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE c/o PESI, P.O. Box 11562-ST, Clayn, Missouri 63105.

Help Wanted

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

I AM COLLECTING the direct (non-toll-free) telephone numbers that will connect directly to the airport airline counters of the following airlines: American, Continental, US Air, Southwest, Delta, Northwest, and United in major cities so that if I am ever bounced or a flight is delayed or canceled, I can reach someone directly and personally with a non 800 number who can do something immediately. The airport airline counter personnel usually know immediately and/or can rebook, etc. without delay. Please email: us.airlines@yahoo.com.

HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to

directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses and acquisitions, as well as general business and corporate law. Over 11 years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

PIMP YOUR WIRELESS ROUTER! http://packetprotector.org. Add VPN, IPS, and web AV capabilities to your wireless router with free, open-source firmware from PacketProtector.org

HACKER TOOLS TREASURE BOX! You get over 650 links to key resources, plus our proven tricks for rooting out the hard-to-find tools, instantly! Use to build your own customized hacker (AHEM, network security) tool kit.
http://FortressDataProtection.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one milltion neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: criminal copyright infringement, unauthorized computer access, theft of trade secrets, identity theft, and trademark infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School, and Gerry Spence's Trial Lawyers College. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600.
http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2007 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

THE HIGH WEIRDNESS PROJECT. We are a SubGenius wiki seeking submissions of strange, controversial, subversive, and above all Slackful sources of information. We do not follow a so-called "neutral point of view" - please make your entries as biased as you want, as long as they're interesting! Special sections dedicated to information warfare, software, conspiracies, religion and skepticism, and more. Check us out: www.modemac.com.

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information, check out: http://www.infosecnews.org.

CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

TRYING HARD not to let the bright light of my mind's eye grow dim. Feed the fire by dropping me a line and filling my head with thoughts. I'll reciprocate by projectile vomiting my intellect straight to your mailbox. Interests include writing, anything computer related, and privacy/anonymity issues. Max Rider, SBI#00383681, DCC 1181 Paddock Rd., Smyrna, DE 19979.

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

ELECTRONIC WARFARE, COUNTERINTELLIGENCE, HACKING. A-Space and Intellipedia are my interests. Looking for pen-pals, friends, and contacts worldwide. I buy books, magazines, and unusual pictures. In search of information on financial privacy, off-shore banking and trusts, unusual books, magazines, and pictures. Please write. English or Spanish OK. Experience in telecom, 2-way radio, packet and advanced threat infrared countermeasures (EW). Former boy, now locked up in one of America's prisons like thousands of other former boys who lost their way. I will respond to all who write. D. Coryell T-68127 D3-247up, PO Box 8504, Coalinga, CA 93210, USA.

OFFLINE OUTLAW IN TEXAS needs some help in developing programming skills. Interested in Perl and Javascript. Also privacy in all areas. Library here is inadequate. Feel free to drop those Bill Me Later cards, add me to the mailing lists, etc.. Thanks to all those who have helped me so much already, you know who you are. William Lindley 822934, CT Terrell, 1300 FM 655, Rosharon, TX 77583-8604

WHEN THE BULLET HITS THE BONE. Bored and lonely phone nerd. Got some time left in our nation's wonderful corrections system. Looking for pen pals to help pass the time. Interests include (not limited to) telecom, computers, politics, music (punk rock, industrial, etc.), tats, urban exploration. 23, white male, 6'1", 190 lbs, black hair, green eyes, a few tats. Will respond to all. Michael Kerr 09496-029, FCI Big Spring, 1900 Simlar Ave., Big Spring, TX 79720.

Advertise in 2600!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600*! Don't even think about trying to tEake out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to: *2600* Marketplace, PO Box 99, Middle Island, NY 11953.

Deadline for Spring issue: 2/25/08.

NEW STUFF!

2600 SWEATSHIRTS - THE SECOND EDITION

We now have a completely new style of hooded sweatshirt in addition to our standard black pullover design. These new ones are gray in color and have a zippered front. Big red numbers proclaim "2600" for those who see you coming and big red letters in the back spell out "HACKER" for those who wonder who it was that just went past. (If you're trying to hide the fact that you're a hacker, this may not be the sweatshirt for you.)

Available in sizes L, XL, and XXL for $35 (outside the U.S. and Canada add $10 for shipping). Send check or money order to address below or visit store.2600.com.
(Additional sizes will be stocked if enough people ask for them.)

THE DIGITAL MILLENNIUM COFFEE MUGS

Yes, you read that right. *2600* now has ceramic coffee mugs designed with the DMCA (Digital Millennium Coffee Act) in mind. The *2600* seal appears on the front and the various restrictions of the mug's use appear on the back. (It is a violation of the DMCA to use this mug for tea.).
2600, PO Box 752, Middle Island, NY 11953 USA

Available with white lettering on a black mug or black lettering on a white mug. $15 each or 2 for $25 (outside the U.S. and Canada add $10 each for shipping - sorry, these things are heavy)

THE LAST HOPE

If you miss this one, there's nothing left to say.

Join us on July 18, 19, and 20, 2008 at the Hotel Pennsylvania in New York City and see who gets the last word.

Special room rates will be available at +1 212 PEnnsylvania 6-5000 (736-5000 for those of you without letters on your phones). Details on who will be speaking and how you can participate along with a whole lot more information is at www.hope.net.

The winner of the Autumn 2007 puzzle is healwhans who correctly surmised that the PDF417 barcode contained a quote from Winston Churchill that was broadcast on October 1, 1939 and said "It is a riddle, wrapped in a mystery, inside an enigma." (He was talking about Russia.)

"First they ignore you, then they laugh at you, then they fight you, then you win." - Mahatma Gandhi

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Mike Castleman

Layout and Design
Skram

Cover
Exscotticus

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Broadcast Coordinators: Juintz, thal

Forum Admin: Skram

IRC Admins: achmet, beave, carton, dukat, enno, faul, koz, mangala, mcfly, r0d3nt, rdnzl, shardy, sj, smash, xi

Inspirational Music: Gigi D'Agostino, Carbon/Silicon, Vienna Vegetable Orchestra, M.I.A.

Shout Outs: Metalab, Odo, Daniele, Bombo, smaster, naif, Luiz, Nelson, Willian, Rodrigo, Johannes, Guenther, Dhillon

Get Well: Jim

Hello: Thomas

2600 *(ISSN 0749-3851, USPS # 003-176); Winter 2007-2008, Volume 24 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $20 individual, $50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate

Back issues available for 1984-2006 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 **Office Line: +1 631 751 2600**
2600 **Fax Line: +1 631 474 2677**

Copyright © 2007-2008; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Ontario

Barrie: William's Coffee Pub, 505 Bryne Dr. 7 pm

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: College Park Food Court, across from the Taco Bell.

Waterloo: William's Coffee Pub, 170 University Ave W. 7 pm

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Exeter: At the payphones, Bedford Square. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tucson: Borders in the Park Mall. 7 pm

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, Wharf #2.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm

Marlborough: Solomon Park Mall food court.

Northampton: Downstairs of Haymarket Cafe. 6:30 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: South Park Mall food court. 7 pm

Raleigh: Royal Bean coffee shop on Hillsboro St (next to the Playmakers Sports Bar and across from Meredith College).

Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Quetzal, 664 Union Ave. 6 pm

Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Charlottesville: Greenberry's Coffee & Tea Company at the Barracks Rd Shopping Center. 6:30 pm

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Barriques Coffee, 127 W Washington Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Overseas Payphones

Iraq. Seen in a bombed out Iraqi hospital east of Baghdad. Note the "Call Me" request on the chassis.

Photo by William Johnson

Iraq. Seen outside a hospital in Sulaimanyah. The white piece of paper gives advice on preventive measures to take so as not to contract cholera.

Photo by Conan

Morocco. Found in Marrakesh, this is what we imagine payphones must look like on other planets.

Photo by birdy

Cayman Islands. This is about as many payphones as you'll ever see in one place. These were found at the port of call for cruise ships in Georgetown, no doubt placed there before the advent of cell phones.

Photo by StankDawg

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo

This photo of 2600 Barracks Road in Charlottesville, Virginia comes to us from Beth Skrobanski. It's home to The Colonnades, a retirement community that we're currently negotiating with to get discounted rates for members of the hacker community when the time comes. Even the font looks familiar.

In answer to the question we get asked more than any other as to just where Walmart Store #2600 is, the answer is of course Chesterfield, Missouri. In fact, it's on the wall of this very store, discovered by Doyle Glaze, that the Children's Miracle Network donated a whole bunch of balloons to commemorate this historic fact.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).